

Symantec™ Network Security User Guide



Symantec Network Security User Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 4.0

Copyright Notice

Copyright © 2004 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, LiveUpdate, Network Security, Symantec Decoy Server, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. Symantec AntiVirus, Symantec Enterprise Security Architecture, and Symantec Security Response are trademarks of Symantec Corporation.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Windows is a registered trademark, and 95, 98, NT and 2002 are trademarks of Microsoft Corporation. Pentium is a registered trademark of Intel Corporation. Sun is a registered trademark, and Java, Solaris, Ultra, Enterprise, and SPARC are trademarks of Sun Microsystems. UNIX is a registered trademark of UNIX System Laboratories, Inc. Cisco and Catalyst are registered trademarks of Cisco Systems, Inc. Foundry is a registered trademark of Foundry Networks. Juniper is a registered trademark of Juniper Networks, Inc. iButton is a trademark of Dallas Semiconductor Corp. Dell is a registered trademark of Dell Computer Corporation. Check Point and OPSEC are trademarks and FireWall-1 is a registered trademark of Check Point Software Technologies, Ltd. Tripwire is a registered trademark of Tripwire, Inc.

Symantec Network Security software contains/includes the following Third Party Software from external sources:

"bzip2" and associated library "libbzip2," Copyright © 1996-1998, Julian R Seward. All rights reserved. (<http://sources.redhat.com/bzip2>).

"Castor," ExoLab Group, Copyright 1999-2001 © 199-2001 Intalio, Inc. All rights reserved. (<http://www.exolab.org>).

Printed in the United States of America. 10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
 - Error messages/log files
 - Troubleshooting performed prior to contacting Symantec
 - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support.

Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Contents

Chapter 1 Introduction

About the Symantec Network Security foundation	9
About the Symantec Network Security 7100 Series	9
About other Symantec Network Security features	11
Finding information	14
About 7100 Series appliance documentation	14
About software documentation	15
About the Web sites	16
About this guide	17

Chapter 2 Architecture

About Symantec Network Security	19
About the core architecture	19
About detection	20
About analysis	24
About response	25
About management and detection architecture	26
About the Network Security console	26
About the node architecture	28
About the 7100 Series appliance node	31

Chapter 3 Getting Started

Getting started	35
About the management interfaces	35
About the Network Security console	36
About management of 7100 Series appliances	38
About user permissions	39
About user passphrases	39
About deployment	40
About deploying single nodes	41
About deploying single Network Security software nodes	41
About deploying single 7100 Series appliance nodes	42
About deploying node clusters	43
Monitoring groups within a cluster	44

Chapter 4 Topology Database

About the network topology	47
Viewing the topology tree	48
Viewing objects in the topology tree	51
Viewing auto-generated objects	51
About location objects	51
About Symantec Network Security objects	52
About router objects	59
About Smart Agents	60
About managed network segments	62
Launching Symantec Decoy Server	63

Chapter 5 Protection Policies

About protection policies	65
Viewing protection policies	66
Understanding the protection policy view	67
Adjusting the view of event types	68
Adjusting the view by searching	68
Adjusting the view by columns	69
Viewing logging and blocking rule details	70
Viewing event detailed descriptions	70
Viewing policy automatic update	70
Annotating policies or events	71

Chapter 6 Response Rules

About response rules	73
About automated responses	74
Viewing response rules	75
Searching event types	76
About response parameters	76
About event targets	76
About event types	77
About severity levels	77
About confidence levels	78
About event sources	78
About response actions	78
About next actions	79
About response actions	79
About no response action	80
About email notification	80
About SNMP notification	80
About TrackBack response action	80

About custom response action	81
About TCP reset response action	81
About traffic record response action	81
About console response action	82
About export flow response action	82
About flow alert rules	83
Viewing flow alert rules	83
Playing recorded traffic	83
Replaying recorded traffic flow data	84

Chapter 7 Detection Methods

About detection	85
About sensor detection	86
Viewing sensor parameters	87
About port mapping	87
Viewing port mappings	87
About signature detection	87
About Symantec signatures	88
About user-defined signatures	88
Viewing signatures	89
About signature variables	89
About refinement rules	89

Chapter 8 Incidents and Events

About incidents and events	91
About the Incidents tab	94
Monitoring incidents	96
Viewing incident data	96
Filtering the view of incidents	98
Monitoring events	99
Viewing event data	99
Filtering the view of events	101
Viewing event notices	102
Managing the incident/event data	103
Loading cross-node correlated events	104
Saving, printing, or emailing incidents	104

Chapter 9 Reports and Queries

About reports	109
Reporting via the Network Security console	109
About report formats	110
About top-level report types	110

- Reports of top events 111
- Reports per incident schedule 112
- Reports per event schedule 113
- Reports by event characteristics 113
- Reports per Network Security device 115
- Drill-down-only reports 116
- About querying flows 117
 - Viewing current flows 117
 - Viewing exported flows 119

Chapter 10 Log Files

- About the log files 121
 - About the install log 121
 - About the operational log 122
- About log files 122
 - Viewing log files 122
 - Viewing live log files 123
 - Refreshing the list of log files 123

Introduction

This chapter includes the following topics:

- [About the Symantec Network Security foundation](#)
- [Finding information](#)

About the Symantec Network Security foundation

The Symantec™ Network Security software and the Symantec Network Security 7100 Series appliance employ a common core architecture that provides detection, analysis, storage, and response functionality. Most procedures in this section apply to both the 7100 Series appliance and the Symantec Network Security 4.0 software. The 7100 Series appliance also provides additional functionality that is unique to an appliance. This additional functionality is described in detail in each section.

This section includes the following topics:

- [About the Symantec Network Security 7100 Series](#)
- [About other Symantec Network Security features](#)

About the Symantec Network Security 7100 Series

Symantec™ Network Security 7100 Series security appliances provide real-time network intrusion prevention and detection to protect critical enterprise assets from the threat of known, unknown (zero-day) and DoS attacks. The 7100 Series appliances employ the new and innovative Network Threat Mitigation Architecture that combines anomaly, signature, statistical and vulnerability detection techniques into an Intrusion Mitigation Unified Network Engine (IMUNE), that proactively prevents and provides immunity against malicious attacks including denial of service attempts, intrusions and malicious code, network infrastructure attacks, application exploits, scans and reconnaissance

activities, backdoors, buffer overflow attempts and blended threats like MS Blaster and SQL Slammer.

In addition to the features it shares with the Symantec Network Security 4.0 software, the Symantec Network Security 7100 Series appliance offers:

- *In-line Operation:* The 7100 Series appliance can be deployed in-line as a transparent bridge to perform real-time monitoring and blocking of network-based attacks. This ability to prevent attacks before they reach their targets takes network security to the next level over passive event identification and alerting. The 7100 Series appliance's One-Click Blocking feature enables users to automatically enable blocking on all in-line interfaces with the click of a single button, saving critical time in the event of worm attacks.
- *Policy-based Attack Prevention:* Deployed in-line, the 7100 Series appliance is able to perform session-based blocking against malicious traffic, preventing attacks from reaching their targets. Predefined and customizable protection policies enable users to tailor their protection based on their security policies and business need. Policies can be tuned based on threat category, severity, intent, reliability and profile of protected resources, and common or individualized policies can be applied per sensor for both in-line and passive monitoring.
- *Interface Grouping:* 7100 Series appliance users can configure up to four monitoring interfaces as an interface group to perform detection of attacks for large networks that have asymmetric routed traffic. A single sensor handles all network traffic seen by the interface group, keeping track of state even when traffic enters the network on one interface and departs on another. This feature greatly increases the attack detection capacity of the 7100 Series and allows it to operate more effectively in enterprise network environments.
- *Dedicated Response Ports:* The Symantec Network Security 7100 Series provides special network interfaces for sending anonymous TCP resets to attackers. With this configuration, network monitoring continues uninterrupted even when sending resets.
- *Reduced Total Cost of Solution:* A single 7100 Series appliance can monitor up to eight network segments or VLANs. The Symantec Network Security 7100 Series reduces the cost of a network security solution by enhancing the security and reliability of the hardware, simplifying deployment and management, and providing a single point of service and support.
- *Flexible Licensing Options:* Each model of the Symantec Network Security 7100 Series offers licensing at multiple bandwidth levels. Whether you

deploy the appliance at a slow WAN connection or on your gigabit backbone, you can select the license that fits your needs.

- *Fail-open:* When using in-line mode, the Symantec Network Security 7100 Series appliance is placed directly into the network path. The optional Symantec Network Security In-line Bypass unit provides fail-open capability to prevent an unexpected hardware failure from causing a loss of network connectivity. The Symantec In-line Bypass Unit provides a customized solution that will keep your network connected even if the appliance has a sudden hardware failure.

See also [“About other Symantec Network Security features”](#) on page 11.

About other Symantec Network Security features

Symantec Network Security is highly scalable, and meets a range of needs for aggregate network bandwidth. Symantec Network Security reduces the total cost of implementing a complete network security solution through simplified and rapid deployment, centralized management, and cohesive and streamlined security content, service, and support.

Symantec Network Security is centrally managed via the Symantec™ Network Security Management Console, a powerful and scalable security management system that supports large, distributed enterprise deployments and provides comprehensive configuration and policy management, real-time threat analysis, enterprise reporting, and flexible visualization.

The Network Security Management System automates the process of delivering security and product updates to Symantec Network Security using Symantec™ LiveUpdate to provide real-time detection of the latest threats. In addition, the Network Security Management System can be used to expand the intrusion protection umbrella using the Symantec Network Security Smart Agents to provide enterprise-wide, multi-source intrusion management by aggregating, correlating, and responding to events from multiple Symantec and third-party host and network security products.

Symantec Network Security provides the following abilities:

- *Multi-Gigabit Detection for High-speed Environments:* Symantec Network Security sets new standards with multi-gigabit, high-speed traffic monitoring allowing implementation at virtually any level within an organization, even on gigabit backbones. On a certified platform, Symantec Network Security can maintain 100% of its detection capability at 2Gbps across 6 gigabit network interfaces with no packet loss.
- *Hybrid Detection Architecture:* Symantec Network Security uses an array of detection methodologies for effective attack detection and accurate attack identification. It collects evidence of malicious activity with a combination

of protocol anomaly detection, stateful signatures, event refinement, traffic rate monitoring, IDS evasion handling, flow policy violation, IP fragmentation reassembly, and user-defined signatures.

- *Zero-Day Attack Detection:* Symantec Network Security's protocol anomaly detection helps detect previously unknown and new attacks as they occur. This capability, dubbed "zero-day" detection, closes the window of vulnerability inherent in signature-based systems that leave networks exposed until signatures are published.
- *Symantec SecurityUpdates with LiveUpdate:* Symantec Network Security now includes LiveUpdate, allowing users to automated the download and deployment of regular and rapid response SecurityUpdates from Symantec Security Response, the world's leading Internet security research and support organization. Symantec Security Response provides top-tier security protection and the latest security context information, including exploit and vulnerability information, event descriptions, and event refinement rules to protect against ever-increasing threats.
- *Real-Time Event Correlation and Analysis:* Symantec Network Security's correlation and analysis engine filters out redundant data and analyzes only the relevant information, providing threat awareness without data overload. Symantec Network Security gathers intelligence across the enterprise using cross-node analysis to quickly spot trends and identify related events and incidents as they happen. In addition, new user-configurable correlation rules enable users to tune correlation performance to meet the needs of their own organization and environment.
- *Full packet capture, session playback and flow querying capabilities:* Symantec Network Security can be configured on a per-interface basis to capture the entire packet when an attack is detected so that you can quickly determine if the offending packet is a benign event that can be filtered or flagged for further investigation. Automated response actions can initiate traffic recording and flow exports, and you can query existing or saved flows as well as playback saved sessions to further assist in drill-down analysis of a security event.
- *Proactive Response Rules:* Contains and controls the attack in real-time and initiates other actions required for incident response. Customized policies provide immediate response to intrusions or denial-of-service attacks based on the type and the location of the event within the network. Symantec Network Security implements session termination, traffic recording and playback, flow export and query, TrackBack, and custom responses to be combined with email and SNMP notifications to protect an enterprise's most critical assets.

- *Policy-Based Detection:* Predefined policies speed deployment by allowing users quickly configure immediate response to intrusions or denial-of-service attacks based on the type and the location of the event within the network. Independently configurable detection settings make it easy for users to create granular responses. Using the robust policy editor, users can quickly create monitoring policies that are customized to the needs of their particular environment. Policies can be applied at the cluster, node, or interface level for complete, scalable control.
- *Role-based Administration:* Symantec Network Security provides the ability to define administrative users and assign them roles to grant them varying levels of access rights. Administrative users can be assigned roles all the way from full SuperUser privileges down to RestrictedUser access that only allows monitoring events without packet inspection capabilities. All administrative changes made from the Network Security console are logged for auditing purposes.
- *TrackBack and FlowChaser:* Symantec Network Security incorporates sophisticated FlowChaser technology that uses flow information from both Network Security software nodes and 7100 Series appliance nodes, and from other network devices to trace attacks to the source.
- *Cost-effective Scalable Deployment:* A single Network Security software node or 7100 Series appliance node can monitor multiple segments or VLANs. Each node can be configured to monitor up to 12 Fast Ethernet ports or 6 to 8 Gigabit Ethernet ports. As the network infrastructure grows, network interface cards can be added to the same node to support additional monitoring requirements.
- *High Availability Deployment:* Network Security software nodes and 7100 Series appliance nodes can be deployed in a High Availability (H/A) configuration to ensure continuous attack detection without any loss of traffic or flow data in your mission-critical environment.
- *Centralized Cluster Management:* A Symantec Network Security deployment can consist of multiple clusters, each cluster consisting of up to 120 nodes, and an entire Network Security cluster can be securely and remotely managed from a centralized management console. The Network Security console provides complete cluster topology and policy management, node and sensor management, incident and event monitoring, and drill-down incident analysis and reporting.
- *Enterprise Reporting Capabilities:* Symantec Network Security provides cluster-wide, on-demand, drill-down, console-based reports that can be generated in text, HTML, and PDF formats and can also be emailed, saved, or printed. In addition, Symantec Network Security provides cluster-wide

scheduled reports generated on the software and appliance nodes that can be emailed or archived to a remote computer using secure copy.

- *Symantec Network Security Smart Agents Technology*: Symantec Network Security Smart Agents enable enterprise-wide, multi-source intrusion event collection, helping companies to expand the security umbrella and enhance the threat detection value of their existing security assets. Third-party intrusion events are aggregated into a centralized location, leveraging the power of the Symantec Network Security correlation and analysis framework, along with the ability to automate responses to intrusions across the enterprise.

See also [“About the Symantec Network Security 7100 Series”](#) on page 9.

Finding information

You can find detailed information about Symantec Network Security software and Symantec Network Security 7100 Series appliances in the documentation sets, on the product CDs, and on the Symantec Web sites.

This section includes the following topics:

- [About 7100 Series appliance documentation](#)
- [About software documentation](#)
- [About the Web sites](#)
- [About this guide](#)

About 7100 Series appliance documentation

The documentation set for the Symantec Network Security 7100 Series includes:

- *Symantec Network Security 7100 Series Implementation Guide* (printed and PDF). This guide explains how to install, configure, and perform key tasks on the Symantec Network Security 7100 Series.
- *Symantec Network Security Administration Guide* (printed and PDF). This guide provides the main reference material, including detailed descriptions of the Symantec Network Security features, infrastructure, and how to configure and manage effectively.
- Depending on your appliance model, one of the following:
 - *Symantec Network Security 7100 Series: Model 7120 Getting Started Card*
 - *Symantec Network Security 7100 Series: Models 7160 and 7161 Getting Started Card*

This card provides the minimum procedures necessary for installing, configuring, and starting to operate the Symantec Network Security 7100 Series appliance (printed and PDF).

- *Symantec Network Security In-line Bypass Unit Getting Started Card* (printed and PDF). This card provides the procedures for installing the optional Symantec Network Security In-line Bypass unit. The bypass unit may be purchased separately from Symantec.
 - *Symantec Network Security 716x Service Manual* (printed and PDF). This document provides instructions for removing the hard drive on the 7160 and 7161.
 - *Symantec Network Security 7100 Series Product Specifications and Safety Information* (printed and PDF). This document provides specifications for all 7100 Series models as well as safety warnings and certification information.
 - *Symantec Network Security User Guide* (PDF). This guide provides basic introductory information about Symantec Network Security core software.
 - *Symantec Network Security 7100 Series Readme* (on CD). This document provides the late-breaking information about the Symantec Network Security 7100 Series, including limitations, workarounds, and troubleshooting tips.
- See also “[Finding information](#)” on page 14.

About software documentation

The documentation set for Symantec Network Security core software includes:

- *Symantec Network Security Getting Started* (printed and PDF): This guide provides basic introductory information about the Symantec Network Security software product, an abbreviated list of system requirements, and a basic checklist for getting started.
- *Symantec Network Security Installation Guide* (printed and PDF): This guide explains how to install, upgrade, and migrate Symantec Network Security software on supported platforms.
- *Symantec Network Security Administration Guide* (printed and PDF): This guide provides the main reference material, including detailed descriptions of the Symantec Network Security features, infrastructure, and how to configure and manage effectively.
- *Symantec Network Security User Guide* (PDF): This guide provides basic introductory information about Symantec Network Security core software.

- *Symantec Network Security Readme* (on CD): This document provides the late-breaking information about Symantec Network Security core software, limitations, workarounds, and troubleshooting tips.
See also “[Finding information](#)” on page 14.

About the Web sites

You can view the entire documentation set on the Symantec Network Security Web site, as well as the continually updated Knowledge Base, Hardware Compatibility Reference, and patch Web sites.

About the Knowledge Base

The *Knowledge Base* provides a constantly updated reference of FAQs and troubleshooting tips as they are developed. You can view the *Knowledge Base* on the Symantec Network Security Web site.

To view the Knowledge Base

- 1 Open the following URL:
http://www.symantec.com/techsupp/enterprise/select_product_kb.html
- 2 Click **Intrusion Detection** > **Symantec Network Security 4.0**.

About the Hardware Compatibility Reference

The *Symantec Network Security Hardware Compatibility Reference* provides a detailed list of platforms supported by Symantec Network Security. You can view the Hardware Compatibility Reference on the Symantec Network Security Web site.

To view the Hardware Compatibility Reference

- 1 Open the following URL:
http://www.symantec.com/techsupp/enterprise/select_product_manuals.html
- 2 Click **Intrusion Detection** > **Symantec Network Security 4.0**.

About the Product Updates site

The *Patch Site* provides downloadable patches as they are released. You can view all available patches on the Symantec Network Security Web site.

To view the Patch Site

- 1 Open the following URL:

http://www.symantec.com/techsupp/enterprise/select_product_updates.html

2 Click **Intrusion Detection** > **Symantec Network Security 4.0**.

See also “[Finding information](#)” on page 14.

About this guide

This guide contains the following chapters:

- Chapter 1 [Introduction](#): Describes the Symantec Network Security intrusion detection system and the Symantec Network Security 7100 Series appliance, documentation, and multiple sources of information.
- Chapter 2 [Architecture](#): Describes the system components, compatibility, and integration of Symantec Network Security and Symantec Network Security 7100 Series appliances.
- Chapter 3 [Getting started](#): Describes basic tasks to start using a Symantec Network Security intrusion detection system.
- Chapter 4 [Topology Database](#)—Describes network topology mapping, and the kind of information visible in the topology database.
- Chapter 5 [Protection policies](#): Describes Symantec Network Security’s protection policies and how to view them.
- Chapter 6 [Responding](#): Describes Symantec Network Security’s response rules and flow alert rules, and how to view them.
- Chapter 7 [Detection Methods](#)—Describes Symantec Network Security’s methods of intrusion, anomaly, and signature detection.
- Chapter 8 [Incidents and Events](#)—Describes detected incidents and their related events, and how to view incident data from the Network Security console.
- Chapter 9 [Reports and Queries](#)—Describes the types of reports that Symantec Network Security can generate and how to generate them.
- Chapter 10 [Managing log files](#): Describes the Network Security log databases and how to view them.

See also “[Finding information](#)” on page 14.

Architecture

This chapter includes the following topics:

- [About Symantec Network Security](#)
- [About the core architecture](#)
- [About management and detection architecture](#)

About Symantec Network Security

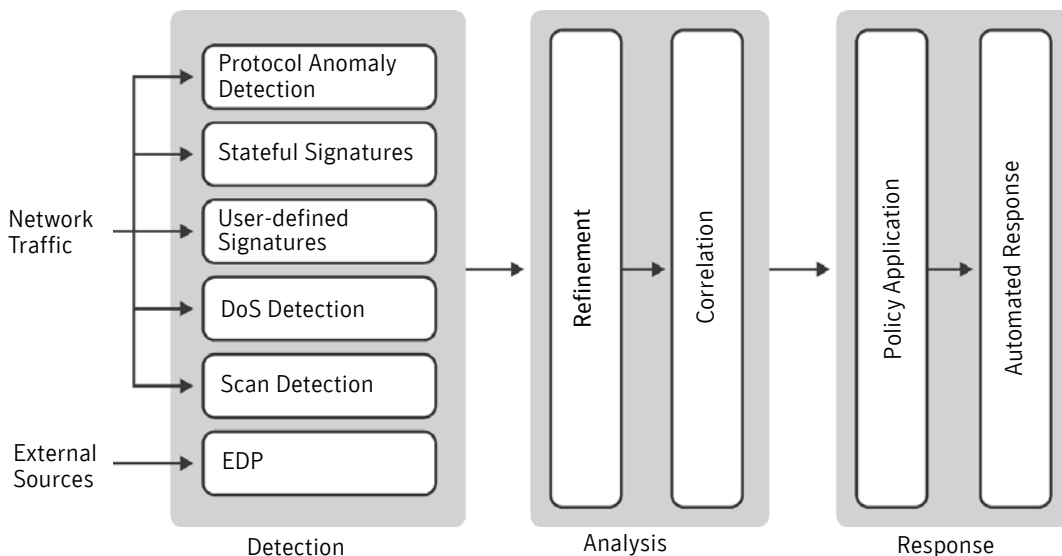
This chapter describes the underlying architecture of both the Symantec Network Security core software and the Symantec Network Security 7100 Series appliances. It describes how the components work together to gather attack information, analyze behavior, and initiate effective responses.

The Symantec Network Security software and the Symantec Network Security 7100 Series appliance employ a common core architecture that provides detection, analysis, storage, and response functionality. Most procedures in this section apply to both the 7100 Series appliance and the Symantec Network Security 4.0 software. The 7100 Series appliance also provides additional functionality that is unique to an appliance. Each section describes this additional functionality in detail.

About the core architecture

Symantec Network Security's challenges are to detect malicious or unauthorized behavior, to analyze the behavior, and to determine an appropriate response. Symantec Network Security provides a three-pronged approach to meet this challenge: detection, analysis, and response. The following diagram describes this basic approach:

Figure 2-1 Core Architecture of Symantec Network Security



This section describes the following topics:

- [About detection](#)
- [About analysis](#)
- [About response](#)

About detection

Symantec Network Security uses multiple methods of threat detection that provide both broad and deep detection of network-borne threats. These include Protocol Anomaly Detection (PAD), traffic rate monitoring, and network pattern matching, or signature-based detection.

Each of these methods has strengths and weaknesses. Signature-based approaches can miss new attacks; protocol anomaly detection can miss attacks that are not considered anomalies; traffic anomaly detection misses single-shot or low-volume attacks; and behavioral anomaly detection misses attacks that are difficult to differentiate from normal behavior.

Symantec Network Security combines multiple techniques and technologies into a single solution. In addition, it adapts to the changing threat landscape by adopting new techniques and technologies that improve upon or replace existing ones.

Users can increase the detection capabilities by using Flow Alert Rules and adding user-defined signatures. Flow alert rules allow users to monitor network policy and respond to traffic to or from IP address and port combinations. User-defined signatures allow users to add network patterns to the supported set, and tune them to a specific network environment. Examples include monitoring proprietary protocols, searching for honey-tokens, or detecting disallowed application versions.

Symantec Network Security can also integrate event data from third-party devices, enabling you to combine existing intrusion detection products with Symantec Network Security's high speed and zero-day attack detection capabilities.

This section describes the layers of the detection model:

- [About protocol anomaly detection](#)
- [About Symantec signatures](#)
- [About user-defined signatures](#)
- [Monitoring traffic rate](#)
- [About DoS detection](#)
- [About external EDP](#)

About protocol anomaly detection

Symantec Network Security's Protocol Anomaly Detection (PAD) is a form of anomaly detection. PAD detects threats by noting deviations from expected activity, rather than known forms of misuse. Anomaly detection looks for expected or acceptable traffic, and alerts when it does not see it. This is the compliment of a signature-based approach, which looks for abnormal, unexpected, or unacceptable traffic.

Symantec Network Security provides in-depth models of the most frequently used network protocols, providing extensive detection capability that goes beyond simpler forms of protocol analysis. These models provide much deeper detection and fewer false positives because they are able to follow a client-server exchange throughout the life of the connection. For example, if a protocol defines the size of a field, and Symantec Network Security detects a field that breaches the defined size, it will trigger an alert.

Symantec Network Security has overcome the issue of overly generic alerts, which is one of the major issues surrounding PAD. During a zero-day attack, a general PAD alert is often all that is possible. However, soon after a new threat is discovered, it is often identified by a name and assigned a unique identifier by authorities. These organizations publish descriptions of the threat and provide

pointers to vendor patches or other remediation tools. When this happens, it is better to have specific threat identification instead of a protocol anomaly alert. Symantec Network Security provides event refinement to address this issue. Threats identified by PAD are further analyzed to determine if they are known or unknown. This processing is done after the traffic has been identified and recorded, so that it does not interfere with the detection performance. This provides the high performance of PAD with the granular identification of a signature matching engine.

About Symantec signatures

Symantec Network Security uses network pattern matching, or signatures, to provide a powerful layer of detection. Signature detection involves detecting threats by looking for a specific pattern or fingerprint of a known bad or harmful thing. This known-bad pattern is called a signature. These patterns are traditionally based on the observed network behavior of a specific tool or tools.

Signature detection operates on the basic premise that each threat has some observable property that can be used to uniquely identify it. This can be based on any property of the particular network packet or packets that carry the threat. In some cases, this may be a literal string of characters found in one packet, or it may be a known sequence of packets that are seen together. In any case, every packet is compared against the pattern. Matches trigger an alert, while failure to match is processed as non-threatening traffic.

Symantec Network Security uses signatures as a compliment to PAD. The combination provides robust detection without the weaknesses of either PAD alone or signatures alone. Symantec Network Security's high performance is maintained by matching against the smallest set of signatures as is possible given the current context. Since many threats are detected and refined through the PAD functionality, Symantec Network Security minimizes the set of required signatures to maximize performance.

Symantec Network Security also uses methods of rapid response in creating signatures that detect attempts to exploit new vulnerabilities as soon as they hit the network, independent of the exploit tool. This results in earlier prevention of threats and more complete coverage.

About user-defined signatures

Symantec Network Security provides the ability to define and apply user-defined signatures to tune Symantec Network Security to your particular environment. User-defined signatures significantly extend the functionality and allow you to leverage the power of Symantec Network Security, such as providing a flexible mechanism for making short-term updates during rapid outbreaks. Symantec Network Security provides an effective way to create,

define, manage, and apply user-defined signatures from the Network Security console.

Monitoring traffic rate

Symantec Network Security detects malicious flow and traffic shape, provides multi-gigabit traffic monitoring, and maintains 100% of its detection capability on a fully saturated gigabit network.

Symantec Network Security performs passive traffic monitoring on its detection interfaces. It uses this data to perform both aggregate traffic analysis and individual packet inspection. Individual packets are inspected and traffic is analyzed per interface. It also uses Netflow data that is locally collected, or forwarded from a remote device, to augment its traffic analysis.

Symantec Network Security's aggregate analysis detects both denial-of-service and distributed denial-of-service attacks. These attacks are recognized as unusual spikes in traffic volume. Using the same data, Symantec Network Security can also recommend proper remediation of the problem.

Beyond attack detection, Symantec Network Security uses traffic analysis to detect many information-gathering probes. It detects not only the common probing methods, but also many stealth modes that slip through firewalls and other defenses. For example, many firewalls reject attempts to send SYN packets, yet allow FIN packets. This results in a common port scan method. Symantec Network Security recognizes this anomaly and triggers an alert.

About DoS detection

Symantec Network Security provides passive traffic monitoring on its detection interfaces that allows it to detect a variety of DoS attacks such as flooding, resource reservation, and malformed traffic. Symantec Network Security also detects a variety of reconnaissance efforts, such as various forms of stealth scans.

About external EDP

The Event Dispatch Protocol (EDP) provides a generalized framework for sending events to software and appliance nodes for correlation, investigation, analysis, and response. Using EDP, Symantec Network Security can collect security data not only from its own sensors, but also from arbitrary third-party sources such as firewalls, IDS sensors, and host-based IDS devices. The process of integrating a third-party sensor generally involves three steps: collection, conversion, and transmission. First, Symantec Network Security collects the data from the third-party sensor in its usual collection format, such as flat text files, SNMP, and source APIs. Then Symantec Network Security converts the

data from the native format to the Symantec Network Security format, and transmits the data to the software or appliance node.

About analysis

Symantec Network Security includes state-of-the-art correlation and analysis that filters out irrelevant information and refines only what is meaningful, providing threat awareness without data overload. Symantec Network Security correlates common events together within an incident to compress and relate the displayed information.

This section describes the analysis mechanism in greater detail:

- [About refinement](#)
- [About correlation](#)
- [About cross-node correlation](#)

About refinement

Symantec Network Security detects both known and unknown (zero-day) attacks, using multiple detection technologies concurrently. Event refinement rules extend the Protocol Anomaly Detection capabilities. Symantec Network Security matches generic anomalies against a database of refinement rules, and for known attacks, reclassifies an anomaly event by retagging it with its specific name.

About correlation

Symantec Network Security uses event correlation, the process of grouping related events together into incidents. This produces a shorter, more manageable list to sift through. Some types of intrusions, such as DDoS attacks, generate hundreds of events. Others, such as buffer-overflow exploits, might generate only one event. Event correlation brings each key event to the forefront in an incident so that it remains visible despite floods of events from other activities. It automates the process of sorting through individual events and frees the user to focus on responding directly to the security incident.

Symantec Network Security correlates security events (intrusions, attacks, anomalies, or any other suspicious activity), response action events (automated actions taken by Symantec Network Security in response to an attack), and operational events (action taken in the administration of the product, such as logging in or rotating logs).

About cross-node correlation

Cross-node correlation is a feature that enables software and appliance nodes in a cluster to communicate with each other and to recognize when similar incidents are monitored by different nodes. Symantec Network Security collects events from both local and remote sources, and organizes the events into a single, rate-controlled stream. It compares new events to existing event groups, and judges similarity. It writes all events and analysis results to a local database, evaluates against protection and response policies, and then takes action if appropriate.

If two peer nodes detect an attack, each node treats it as a separate incident and has no knowledge of what the other node detects. However, when Symantec Network Security applies cross-node correlation to the incidents detected by two nodes in a cluster, each adds a reference to the other and maintains awareness that this may be the same or a related attack. The Network Security console displays both as a single incident.

About response

Protection policies and response rules are collections of rules configured to detect specific events, and to take specific actions in response to them. Protection policies can take action at the point of detection. Using a 7100 Series appliance, you can configure Symantec Network Security to block events before they enter the network. Response rules can be configured to react automatically and immediately contain and respond to intrusion attempts.

The response mechanism is described further in the following sections:

- [About protection policies](#)
- [About response rules](#)

About protection policies

Symantec Network Security applies protection policies to interfaces at the point of detection, before they enter the network. Each protection policy indicates the specific signatures that the sensor will hunt for on the applied interface, in addition to protocol anomaly detection events. If a 7100 Series appliance is deployed in-line, it can use blocking rules to prevent traffic from entering the network.

About response rules

Symantec Network Security's automated rule-based response system includes alerting, pinpoint traffic recording, flow tracing, session resetting, and custom responses on both the software and appliance nodes and the Network Security

console. Symantec Network Security generates responses based on multiple criteria such as event targets, attack types or categories, event sources, and severity or confidence levels. Multiple responses can be configured for the same event type, as well as the order in which Symantec Network Security executes the responses.

Symantec Network Security reviews each event, and iterates through the list of response rules configured by the user. It compares each event against configurable match parameters. If a match occurs on all parameters, it then executes the specified action. After Symantec Network Security processes one rule, it proceeds to one of three alternatives: to the rule indicated by the Next parameter, to a following rule beyond the Next rule, or it stops policy application altogether for this event.

About management and detection architecture

Symantec Network Security combines two main physical components: management and detection. The management component, called the Network Security console, provides management functionality such as incident review, logging, and reporting. The detection component is available as a Network Security software node or a Symantec Network Security 7100 Series appliance node. Both are based upon the same basic architecture, and both provide detection, analysis, storage, and response functionality. The 7100 Series node includes the functionality of the Network Security software node, with additional unique functionality.

This section describes the following components in greater detail:

- [About the Network Security console](#)
- [About the node architecture](#)
- [About the 7100 Series appliance node](#)

About the Network Security console

Symantec Network Security's administrative and management component is the powerful but easy-to-use Network Security console. It communicates over an encrypted and authenticated link to ensure that authorized administrators may log in from any secure or insecure network. The Network Security console manages all operations, including incident and event filtering, drill-down incident analysis, full packet capture, detailed event descriptions, and allows event annotations and incident marking for tracking.

The Network Security console provides an interface from which you can monitor events and devices, edit parameters, configure response rules, apply

protection policies, and view log data. You can generate reports and view them immediately in the Network Security console, or you can schedule them to generate automatically.

The Network Security console contains three main tabs that provide a view of the Devices tab, Incidents tab, and Policies tab.

- **Devices tab:** Provides a hierarchical tree view of the network topology, with a detailed summary of each device.
- **Incidents tab:** Provides detailed descriptions of incidents and events taking place in the monitored network, and can be drilled down to reveal detailed packet information.
- **Policies tab:** Provides the tools to create, manage, and apply user-defined signatures, signature variables, and protection policies.

Reporting in the Network Security console includes dynamic chart and graph generation, with information drill-down and data retrieval. Pre-defined reports can be saved and printed. Users can send flow queries and play back traffic sequences from the Network Security console as well.

About role-based administration

The Network Security console provides a simple yet powerful interface that is useful for all levels of administration, from the Network Operation Center (NOC) operator who watches for a red light, to the skilled security administrator who examines and analyzes packets.

Four pre-defined user groups provide efficient management. Each group includes a set of permissions for specific management operations. Each user's login identity indicates their role and permission assignment during an administrative session.

Symantec Network Security automatically installs a SuperUser login account that is authenticated with full administrative capabilities. The SuperUser can create additional login accounts in the following user groups:

- *SuperUsers:* A user authenticated with full administrative capabilities. This user is allowed to perform all administrative tasks that the Network Security console can execute.
- *Administrators:* A user authenticated with partial administrative capabilities. This user is allowed to perform most administrative tasks, with the exception of some advanced actions.
- *StandardUsers:* A user authenticated with full read-only capabilities. This user is allowed to view all information in the Network Security console.

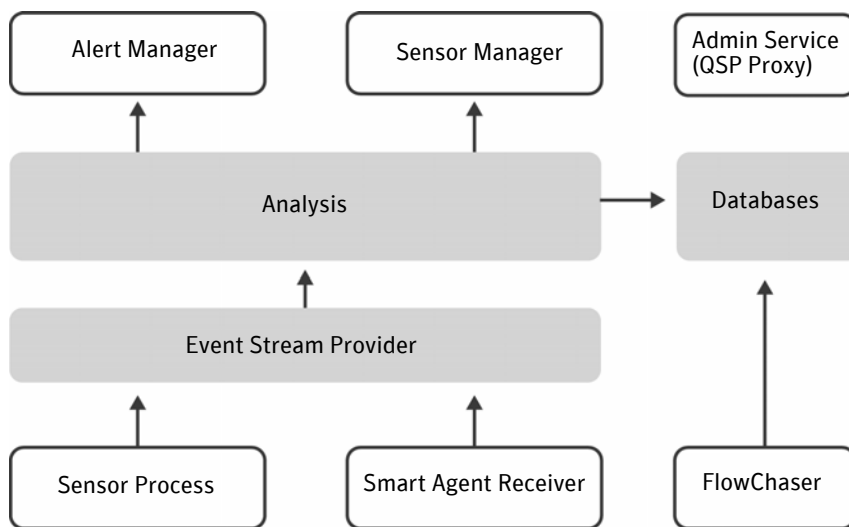
- *RestrictedUsers*: A user authenticated with partial read-only capabilities. This user is allowed to view most information in the Network Security Console with the exception of some advanced information and network-sensitive data.

About the node architecture

The Network Security software node or 7100 Series appliance node contains a variety of tools and techniques that work together to gather attack information, analyze the attacks, and initiate responses appropriate to specific attack circumstances.

The following diagram illustrates how Symantec Network Security's arsenal of tools work together to provide protection:

Figure 2-2 Core architecture of a software or appliance node



The components of the core node architecture apply to both Network Security software nodes and 7100 Series appliance nodes as follows:

- [About the alert manager](#)
- [About the sensor manager](#)
- [About the administration service](#)
- [About analysis](#)
- [About the databases](#)
- [About Event Stream Provider](#)

- [About sensor processes](#)
- [About Smart Agents](#)
- [About FlowChaser](#)

About the alert manager

The Network Security Alerting Manager provides three types of alerts: a Network Security console action alert, an email alert, and an SNMP trap alert.

About the sensor manager

The Sensor Manager maintains a pool of sub-processes to manage sensor-related functionality. This includes sensor processes for event detection, traffic recording, and FlowChaser sub-processes that handle network device configuration, starting, and stopping.

About the administration service

All communication across the network passes through the QSP Proxy, an administration service with 256-bit AES encryption and passphrase authentication. This ensures that all communication between the Network Security console and the master node, and between software and appliance nodes within a cluster, are properly authenticated and encrypted. In addition, this service enforces role-based administration and thus prevents any circumvention of established access policy.

About analysis

Symantec Network Security's analysis framework aggregates event data on possible attacks from all event sources. The analysis framework also performs statistical correlation analysis on events to identify event patterns that vary significantly from usual network activity and to identify individual events that are highly related, such as a port scan followed closely by an intrusion attempt.

About the databases

Symantec Network Security provides multiple databases to store information about attacks, the network topology, and configuration information.

- *Topology database:* Stores information about local network devices and interfaces and the network configuration. Symantec Network Security uses this data to direct the FlowChaser toward the area of the network in which an attack occurs.

- *Protection policy database*: Stores the pre-defined protection policies that installed with the product and those added through LiveUpdate, as well as any user-defined signatures.
- *Response rule database*: Stores the rules that define the actions to take when an attack is identified, the priority to give to the attack incidents, and the necessity for further investigation of the attack.
- *Configuration database*: Stores configurable parameters that SuperUsers and Administrators can use to configure tasks at the node level and to configure detection at the sensor level.
- *Incident and event databases*: Stores information about events and incidents. The event log can be signed periodically by the iButton or soft token to verify that the log has not been tampered with or altered in any way. The iButton is a hardware device that safeguards the signature certificate and confirms the identity of a Network Security software node.
- *LiveUpdate database*: Stores data relevant for LiveUpdate.
- *User database*: Stores information about each user login account.

About Event Stream Provider

The Event Stream Provider (ESP) prevents event flood invasions by intelligently processing them in multiple event queues, based on key criteria. In this way, if multiple identical events bombard the network, the ESP treats the flood of events as a single unit. This prevents any one event type or event source from overloading a security administrator. Thus, the events that are forwarded are representative of the actual activity on the network. If it is necessary to drop events for stability and security, the ESP does so in a manner that loses as little important information as possible.

If a second attack is hidden beneath the volume of an event flood attack, the events related to the hidden attack will differ from the flood events. Therefore, the ESP places these events in separate queues. The analysis framework can then analyze the events related to the hidden attack. In this way, Symantec Network Security analyzes and responds to both attacks quickly and effectively.

About sensor processes

Symantec Network Security sensors can operate using in-line or passive mode, and using interface groups or single monitoring interfaces. In-line deployment and interface groups are possible using a Symantec Network Security 7100 Series appliance only.

Independent of the deployment mode of a particular sensor, Symantec Network Security applies the same comprehensive detection strategy and protection,

tuned to maximize detection while retaining network performance and reliability. For example, using in-line mode, the sensor tunes itself to minimize latency and maximize throughput across a pair of interfaces. Using interface groups, the sensor correctly adjusts itself to compensate for the fact that a single network session may be conducted using multiple, asymmetric links. Using single monitoring interfaces, the sensor batches process packets to maximize detection coverage.

About Smart Agents

Symantec Network Security Smart Agents® (Smart Agents) combine an investment in first-generation network intrusion detection products with Symantec Network Security's high speed and zero-day attack detection capabilities. Using Smart Agents as the bridge between Symantec Network Security and other intrusion detection and firewall products, users can centralize management of events and incidents from the Network Security console.

Smart Agents enable Symantec Network Security to collect data from third-party hosts and network IDS products in real time. Smart Agents collect event data from external sensors such as Symantec Decoy Server®, as well as from third-party sensors, log files, SNMP, and source APIs. They send this data to be analyzed, aggregated, and correlated with all other Symantec Network Security events.

About FlowChaser

FlowChaser serves as a data source in coordination with TrackBack, a response mechanism that traces a DoS attack or network flow back to its source, or to the edges of an administrative domain. FlowChaser receives network flow data from multiple devices, such as Network Security sensors and network routers. FlowChaser stores the flow data in an optimized fashion that enhances analysis, correlation, and advanced responses.

About the 7100 Series appliance node

The Symantec Network Security 7100 Series is a dedicated, scalable appliance designed to monitor and protect multiple network segments at multi-gigabit speeds using Symantec Network Security software. The appliance provides advanced intrusion detection and prevention on enterprise-class networks. The Symantec Network Security 7100 Series runs an optimized, hardened operating system with limited user services to further increase security and performance.

The appliance provides all the functionality of a Network Security software node, with additional capabilities in the areas of detection, response, and management.

This section describes the following topics:

- [About detection on the 7100 Series](#)
- [About response on the 7100 Series](#)

About detection on the 7100 Series

In addition to the detection facilities of Symantec Network Security software, the 7100 Series appliance provides a new detection feature called interface grouping.

About interface grouping

Interface grouping, also called port clustering, enables up to four monitoring interfaces to be grouped together as a single logical interface. This is especially useful in asymmetrically routed environments, where incoming traffic is seen on one interface and outbound traffic passes through another. Grouping the interfaces into one logical interface with a single sensor allows state to be maintained during the session, making it possible to detect attacks.

About response on the 7100 Series

An important new 7100 Series response capability is provided by the addition of in-line monitoring mode.

About in-line monitoring mode

In-line monitoring mode places the full capabilities of the Symantec Network Security 7100 Series directly into the network path, enabling you to detect and block malicious traffic before it enters your network. With an active sensor monitoring traffic on an in-line interface pair, all packets are examined in real time so that you can prevent intrusions from reaching their targets. By comparison, passive mode supplies monitoring, alerting, and response capabilities, while in-line mode provides all these plus proactive intrusion prevention.

About blocking or alerting mode

In-line mode protection policies are configurable so that you can choose to block and alert on designated events. You can easily switch between blocking and alerting in the Network Security console.

In blocking mode, all network traffic is examined by the Network Security detection software before it enters your network, and is blocked if malicious. When a protocol anomaly event or an event matching an enabled signature is detected, the offending packet is dropped. For TCP/IP traffic, a reset is sent to the TCP connection.

In alerting mode, the Network Security detection software still analyzes all packets as they enter your network, but does not prevent an intrusion attempt from proceeding. You can configure a non-blocking protection policy to send a reset and an alert, based on event ID.

With only alerting enabled under in-line mode, there is no risk of inadvertently blocking legitimate network traffic. The advantage of in-line alerting mode over operating in passive mode is that you can enable blocking with a single mouse-click from the Network Security console. You don't need to halt network traffic while changing cabling and configuration to switch between in-line alerting and blocking modes.

About fail-open

When you configure in-line mode on the Symantec Network Security 7100 Series appliance, you place the in-line interface pair directly into the network path. If the appliance or one of those interfaces has a hardware or software failure, all associated network traffic is blocked. You can avoid this risk with the addition of the 2 In-line Bypass unit or 4 In-line Bypass unit, custom fail-open devices available from Symantec specifically for the appliance. These devices provide the fail-open capability, allowing your network to stay up while you make repairs.

At this time, the bypass units are only available for copper interfaces. There is currently no fail-open solution for the fiber interfaces of the appliance model 7161.

Getting Started

This chapter includes the following topics:

- [Getting started](#)
- [About the management interfaces](#)
- [About user permissions](#)
- [About deployment](#)
- [About deploying single nodes](#)
- [About deploying node clusters](#)

Getting started

This chapter provides a general outline of major tasks involved in setting up a core Symantec Network Security intrusion detection system. It describes basic tasks, including accessing the management interfaces (Network Security console, serial console, and LCD panel), accessing nodes and sensors, and establishing user permissions and access. It also describes most often used deployment scenarios.

About the management interfaces

Symantec Network Security provides a management interface called the Network Security console. Both the Symantec Network Security software and the 7100 Series appliance utilize the Network Security console for the majority of tasks. Users can also use a serial console or LCD panel for initial configuration of the 7100 Series appliance.

About the Network Security console

The Network Security console serves as the main management interface for both Network Security software nodes and 7100 Series appliance nodes. The Network Security console uses QSP 256-bit AES encryption.

This section describes how to launch the Network Security console and adjust the view:

- [Launching the Network Security console](#)
- [Viewing the Network Security console](#)
- [Adjusting the Devices view](#)
- [Adjusting the Incidents view](#)
- [Viewing node status](#)

Caution: The first time you launch the Network Security console after installation, expect a wait time of a few minutes while the database files load. Symantec Network Security caches the files after that first load, and makes subsequent launches faster.

Launching the Network Security console

All users can launch the Network Security console on Windows, Solaris, and Linux, and view the main tabs and menus.

To launch the Network Security console

- 1 Depending on the operating system, do one of the following:
 - For Windows, double-click the **Symantec Network Security** icon on the desktop.
 - For Solaris or Linux, run the following command:
`<path to java>/bin/java -Xmx256M -jar snsadmin.jar`
For example:
`/usr/SNS/java/jre/bin/java -jar snsadmin.jar`

Note: The Network Security console must have Java 1.4 installed to run.

- 2 In **Hostname**, enter the hostname or IP address of the software or appliance node you want to monitor.
- 3 In **Port**, enter the port number.
If in a cluster, all nodes must use the same port number.

- 4 In **Username**, enter the user name. Access and permissions depend on the user group of your login account.
- 5 In **Passphrase**, enter the passphrase established for your user login account, and click **OK**.

Caution: If a non-SuperUser uses the wrong passphrase, an **Incorrect Username or Passphrase** message appears. If this occurs multiple times (as specified by the Maximum Login Failures parameter), the Network Security console locks the non-SuperUser out. Even if the correct passphrase is used at that point, access is denied. Contact the SuperUser to create a new passphrase.

Viewing the Network Security console

The Network Security console contains three main tabs that provide a view of the network topology, the network traffic, and the detection and response functionality:

- The **Devices** tab provides a hierarchical tree view of the network topology with a detailed summary of each device.
- The **Incidents** tab provides detailed descriptions of security incidents and their correlated events taking place in the network, including sub-levels of packet detail.
- The **Policies** tab provides the area for managing protection policies and automated responses at the point of entry.

Adjusting the Devices view

You can adjust the display of the network topology tree in the Devices tab as follows:

To display the entire topology tree

- In the **Devices** tab, click **Topology** > **Expand All Objects**.

To display all device objects and hide all interface objects

- In the **Devices** tab, click **Topology** > **Expand Categories**.

To display the first level of objects in the topology tree

- In the **Devices** tab, click **Topology** > **Collapse All Objects**.

Adjusting the Incidents view

You can adjust the display of the events and incidents tables in the Incidents tab as follows:

To adjust the font size of the display

- In the **Incidents** tab, click **Configuration > Table Font Size > OK**.

Adjusting the Policies view

You can adjust the display of the list of event types in the Policies tab, to view a workable subset. To do this, see [“Adjusting the view of event types”](#) on page 68.

Viewing node status

The Network Security console displays an object in the topology tree representing devices and interfaces in the network. When a software or appliance node experiences a process failure of any kind, the Network Security console displays the node with a red X, called the Node Status Indicator. This signifies that Network Security processes or connectivity to the network has failed.

To view node status

- ◆ See the **Node Status Indicator** for the software or appliance node.
A red X or Node Status Indicator signifies that Network Security processes or network connectivity failed on a software or appliance node.



About management of 7100 Series appliances

Users can also use a serial console or LCD panel for initial configuration of the 7100 Series appliance, as well as the Network Security console.

About the LCD panel

The Symantec Network Security 7100 Series appliance is equipped with an LCD screen and push buttons on the front bezel. The screen can display two lines of sixteen characters each, and there are six buttons: four arrow buttons and two function buttons labeled **s** (start) and **e** (enter).

You can use the LCD panel for initial configuration of your appliance. After initial configuration, the LCD screen displays system statistics in a rotating sequence, and provides a menu of tasks including stopping and starting Symantec Network Security, rebooting or shutting down the appliance, and changing the IP address.

About the serial console

You can use the serial console for initial configuration of the appliance and for command line access to the operating system utilities and filesystems. The serial console provides an alternative to using the LCD panel for initial configuration.

Serial console access requires a valid username and password.

Note: See the *Symantec Network Security 7100 Series Implementation Guide* for more information about the serial console and LCD panel.

About user permissions

Symantec Network Security provides an efficient way to administer user access using four predefined groups: SuperUser, Administrator, StandardUser, and RestrictedUser. The installation procedure creates one user login account in the SuperUser group with full access and all permissions. At any time after installation, this SuperUser can create additional user login accounts in any of the four groups, from the Network Security console. Each group includes a predefined set of permissions and access that cannot be modified.

Note: The four user groups are unique to the Network Security console and do not extend to the serial console or the LCD panel. See the *Symantec Network Security 7100 Series Implementation Guide* for more information about the serial console and LCD panel.

About user passphrases

The SuperUser password for a master 7100 Series node is entered during the initial configuration of the appliance. This password is used for the Network Security console login, root login, secadm login, and for unlocking the LCD panel. For security reasons, we recommend that you change passwords periodically for the root, secadm, and Network Security console user login accounts.

Symantec Network Security provides an efficient way to control access to the Network Security console for both software and appliance nodes by managing user passphrases.

The passphrase identifies each user with a user group that includes a predefined set of permissions and access. All users can change their own passphrase at any time.

To change login account passphrases

- 1 In the Network Security console, click **Admin > Change Current Passphrase**.
- 2 In **Change Passphrase for <user>**, enter the existing passphrase.
- 3 Enter a new passphrase from 6 to 16 characters, inclusive, and confirm it.
- 4 Click **OK** to save and close.

Note: If a non-SuperUser uses an incorrect passphrase, an **Incorrect Username or Passphrase** message appears. If this happens multiple times (as specified by the Maximum Login Failures parameter), the user can be locked out. Even if the correct passphrase is used at that point, access is denied. Contact the SuperUser to create a new passphrase.

Note: Both StandardUsers and RestrictedUsers can modify their own passphrases, but cannot add, edit, or delete those of other users.

About deployment

Both software and appliance nodes can be deployed singly or clustered:

- **Single-node deployment:** A peer relationship between one or more individual single nodes, viewed from one or more independent Network Security consoles.
- **Cluster deployment:** A hierarchical relationship between one master node and up to 120 slave nodes that synchronize to the master node.

Both software and appliance nodes can be deployed using passive mode; only 7100 Series appliances can be deployed using in-line mode:

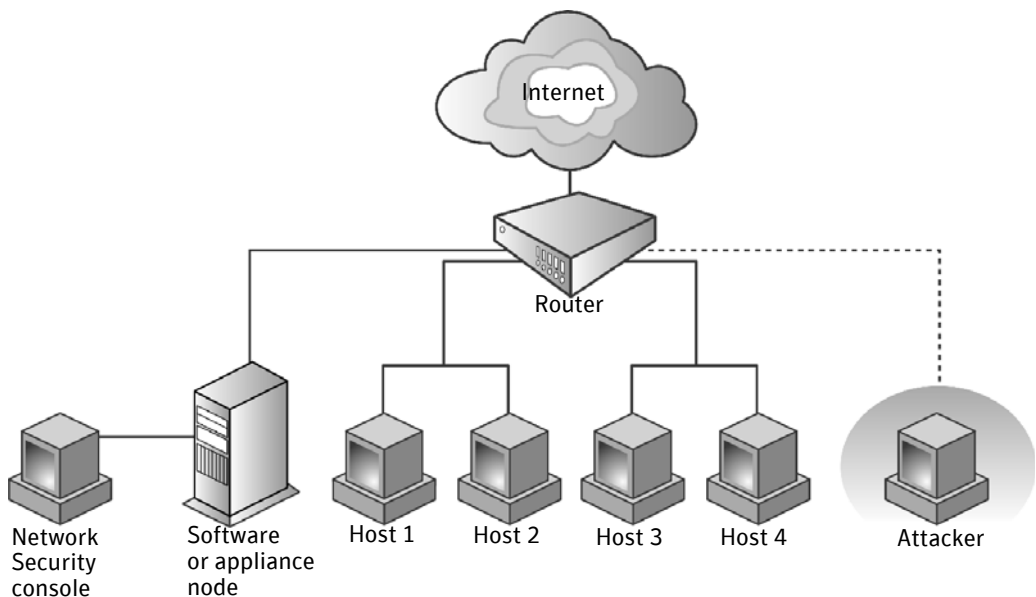
- **In-line deployment:** Only the Symantec Network Security 7100 Series appliance can be deployed in-line at this time. In-line mode enables multiple features such as the ability to block specified traffic from entering the network.
- **Passive deployment:** Both software and appliance nodes can be deployed in passive mode, and positioned near the network, where they do not impede network performance as a point of failure. No service is ever lost, even if the node fails. The possibility of failure can be mitigated by failover groups that maintain the availability of all nodes.

About deploying single nodes

Symantec Network Security can be deployed as one or more single nodes that operate independently of each other within your network. This section describes both Network Security software nodes and 7100 Series appliance nodes deployed in this manner.

This figure shows the relationship between a fictitious network, a single software or appliance node, and a possible intruder:

Figure 3-1 Fictitious Network Map with Intruder



About deploying single Network Security software nodes

Symantec Network Security can be deployed using one or more single Network Security software nodes. Each node functions independently as the master node in a cluster of one.

Managing a single node is simpler than managing a cluster. For example, you can partition your network to make each security administrator responsible for only one segment, without the need to communicate with other segments or with other software or appliance nodes. In this scenario, the nodes have no method of communication with each other. Using a single Network Security console, you can log in to any single node in your network, and view it individually. With single-node deployment, users cannot view all nodes

simultaneously from the Network Security console. Also, failover groups do not function for single nodes.

About deploying single 7100 Series appliance nodes

You can deploy a Symantec Network Security 7100 Series node just as you would a Network Security software node. It can operate independently or as part of a cluster. A 7100 Series appliance also has several extra deployment options. You can configure it for interface grouping, in-line mode, and fail-open, in addition to passive monitoring mode. You can also deploy the appliance using a combination of these modes in a way that best suits your network.

About interface grouping

Interface grouping provides a solution when your network employs asymmetric routing. Asymmetric routing occurs when traffic arrives on one interface and departs on another. Because the request and reply sides of the client/server traffic are on different interfaces, a standard monitoring interface cannot see the full conversation to analyze it properly. With the Symantec Network Security 7100 Series, you can place up to four interfaces into a single group. One sensor is started for the interface group, allowing Symantec Network Security to analyze the different traffic flows as if they were combined on one interface. This is a very effective deployment mode for a network with asymmetric routing.

About in-line mode

In-line mode is another mode of deployment available only with the Symantec Network Security 7100 Series appliance. In-line mode uses an interface pair to place the appliance directly into the network path. Both interfaces connect to the monitored network segment, effectively separating it into two sides. Incoming packets are fully analyzed before being allowed to continue into the other side of the network. Because of the nature of the connection, it is necessary to interrupt network traffic briefly while you connect the cables to the appliance interfaces.

You can configure a policy for an in-line pair that alerts on or blocks malicious traffic. When a malicious packet is detected in alerting mode, the appliance software executes the configured responses, which may be email, Network Security console displays, or other choices available on both appliances and Network Security software nodes. Blocking mode prevents malicious traffic of the designated event types from being transmitted into your protected network. When a blocked TCP/IP event is detected, the node sends TCP resets to both

interfaces in the pair. For a blocked UDP event, the appliance drops the packet and marks the flow as dropped.

For policies configured with both blocking and alerting, you can run Network Security with blocking disabled until you are sure the policy is correct. If you decide that the configured event types should be blocked, you can change the policy to enable blocking with a single mouse-click in the Network Security console.

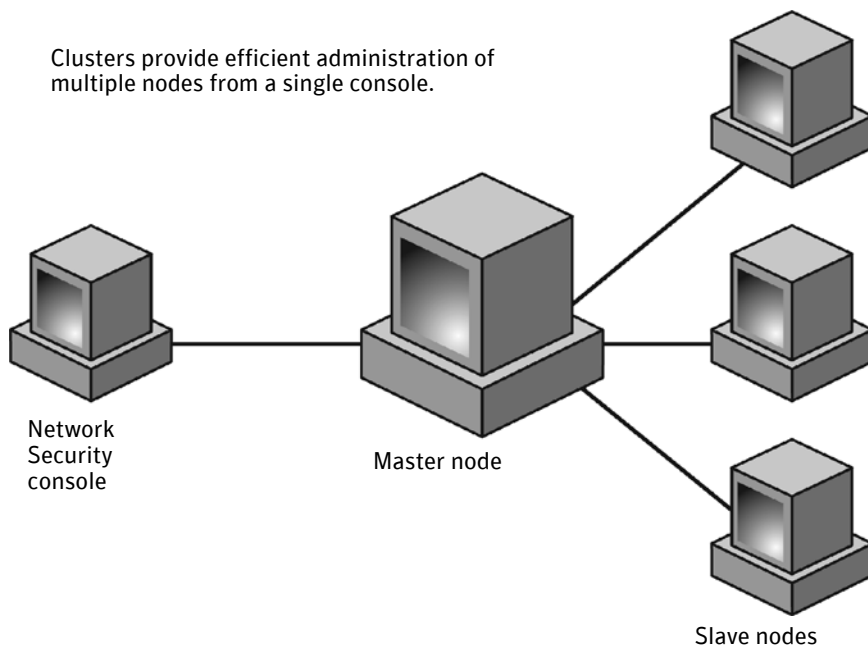
About fail-open

Fail-open is an option when using in-line mode and is the default for passive mode. Fail-open means that if the appliance has a hardware failure, network traffic will continue. Since the Symantec Network Security 7100 Series appliance is directly in the network path while deployed using in-line mode, fail-open capability requires the purchase and installation of a separate device. The Symantec Network Security In-line Bypass unit has been custom designed to provide fail-open capability for the Symantec Network Security 7100 Series. The bypass unit is available in two models, which accommodate two or four in-line interface pairs respectively. Fail-open is available for all copper gigabit or Fast Ethernet interfaces on the appliance. It is not an option for fiber interfaces at this time. The In-line Bypass unit is only necessary for fail-open when appliance interfaces are configured for in-line mode. All interfaces configured in passive mode are fail-open by default.

About deploying node clusters

The full power and advanced features of Symantec Network Security become available when you create a group or cluster of nodes, and establish one node as the master. A cluster of software or appliance nodes enables Symantec Network Security to monitor all parts of a network from the central Network Security console, and share information between nodes. In a clustered deployment, the master node can check, update, and synchronize all nodes in the cluster. High-availability failover deployment becomes available using pair configurations of active and standby nodes. Users can view all Network Security

software nodes and 7100 Series appliance nodes in your network simultaneously, and make full use of advanced capabilities.



Monitoring groups within a cluster

The Network Security console provides a way to subdivide a cluster into different monitoring groups. You can then configure the Network Security console to display only the incidents of selected monitoring groups. In this way, you can manage the delegation of responsibilities in a large installation where each operator is responsible for only a subset of software or appliance nodes. This increases performance as well, because it reduces the number of incidents that a single Network Security console must load.

When subdivided by monitoring groups, Symantec Network Security continues to perform cross-node correlation across all nodes in the cluster, even though the Network Security console displays incidents only from the subset.

Selecting a monitoring group

Symantec Network Security provides a way to display a subset of the incident list focused on only those software or appliance nodes that are included in the selected monitoring group.

To focus the incident view on a monitoring group

- 1 In the Network Security console, click **Configuration > Monitoring Groups**.
- 2 In **Choose Monitoring Groups**, select a group or check **Default**.
- 3 Click **OK** to view incidents from the selected monitoring group.

Note: Always assign at least one node to each monitoring group. If you create groups without assigning nodes to them, you can miss events even though the sensors detect them. In other words, you can inadvertently hide your view of the events by creating groups that you do not use.

Note: Both StandardUsers and RestrictedUsers can choose monitoring groups, but cannot add, edit, or delete them.

Topology Database

This chapter includes the following topics:

- [About the network topology](#)
- [Viewing objects in the topology tree](#)
- [Viewing the topology tree](#)
- [Launching Symantec Decoy Server](#)

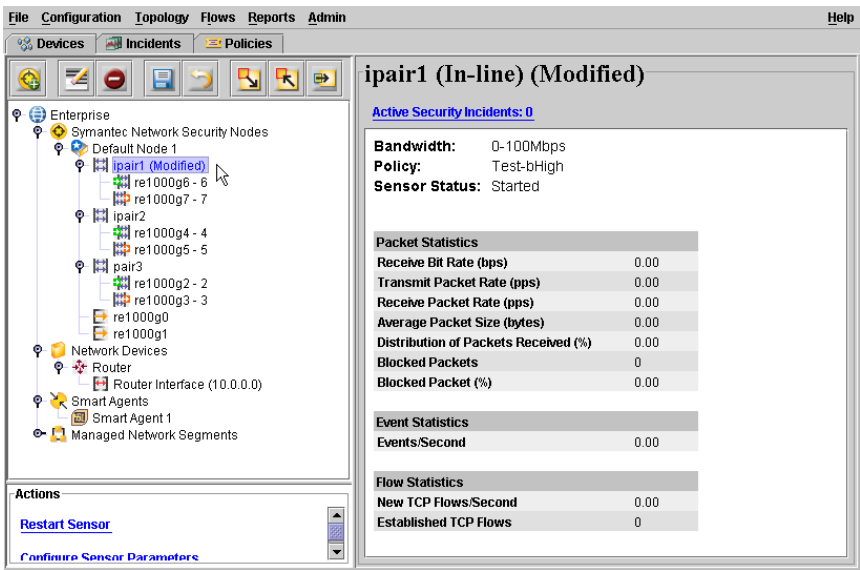
About the network topology

The Network Security console displays the topology tree on the Devices tab. The topology tree represents the elements of your network, and provides Symantec Network Security with the necessary information about the topology of the network or portion of the distributed network that it monitors. Network Security also requires information about connections to autonomous systems or other segments within a distributed network.

Note: Both StandardUsers and RestrictedUsers can view the topology tree displayed on the Devices tab, but cannot modify it.

The Network Security console displays the network topology as a hierarchical tree structure. At a glance, you can see a representation of each network location, network segment, and router in your network, as well as the 7100 Series appliance nodes and/or Network Security software nodes and interfaces that monitor your network. The installation process generates some objects automatically. Security administrators can add the others, providing Symantec Network Security with the information it needs to monitor your network.

The following figure shows an example:



Viewing the topology tree

The topology tree can be modified at any time to adjust to new information, to network reorganization, or to make other network changes. This section describes how to view object information, refresh the topology tree view, and to check the status of an individual Network Security software node.

Types of objects

The Devices tab displays the following types of objects to represent the elements of your network and security system:

- **Locations:** Objects that represent physical or logical groups of one or more network segments. The installation procedure automatically creates the first location object, named Enterprise by default.
- **Symantec Network Security nodes:** The object category for both software and appliance nodes.
 - **Software nodes:** Objects that represent the Symantec Network Security software installed on a designated computer.
 - **7100 Series nodes:** Objects that represent the Symantec Network Security 7100 Series appliances.
- **Network devices:** The object category for both routers and router interfaces.

- **Routers:** Objects that represent devices that store data packets and forward them along the most expedient route. Symantec Network Security monitors this connection between hosts or networks.
- **Interfaces:** Objects that represent boundaries across which separate elements can communicate. Interfaces provide the point of contact between Symantec Network Security and routers.
- **Smart Agents:** Objects that represent the entry point for event data from Symantec Decoy Server, Symantec Network Security Smart Agents, and other third-party sensors.
- **Managed network segments:** Objects that represent subnets in which the network devices and interfaces reside. The Network Security console automatically creates a network segment object for each unique subnet.
- **Interfaces:** Objects that represent boundaries across which separate elements can communicate. Interfaces provide the point of contact between Symantec Network Security and your network devices.
 - **Monitoring interfaces:** Objects that represent dedicated ports that mirror incoming or outgoing traffic on a software or appliance node.
 - **In-line pairs:** Objects that represent pairs of interfaces on a 7100 Series appliance node that are directly in the network traffic path. For a given flow, one interface connects to inbound traffic and the other to outbound traffic. Only in-line pairs can be configured to block malicious traffic.
 - **Interface groups:** Objects that represent groups of two to four interfaces on a 7100 Series appliance node that share a common sensor. Interface groups are used to monitor asymmetrically routed network environments, and are configurable only on 7100 Series nodes.

Viewing node status

The Network Security console displays an object in the topology tree representing devices and interfaces in the network. When a software or appliance node experiences a process failure of any kind, the Network Security console displays the node with a red X, called the Node Status Indicator. This signifies that Network Security processes or connectivity to the network has failed.

To view node status

- ◆ See the **Node Status Indicator** for the software or appliance node.



A red X or Node Status Indicator signifies that Network Security processes or network connectivity failed on a software or appliance node.

Viewing node details

When you click an object in the topology tree, the Network Security console displays the description, if applicable, and other pertinent details about the software or appliance node, such as its IP address or subnet mask.

To view node details

- ◆ Click the corresponding device object.
The Network Security console displays the details and optional description in the right pane.

Viewing object details

When you select an object in the Devices tab, the right pane displays information about that object. Depending on the selected object, the following information can appear in the right pane:

- **Device Type:** Displays the type of device selected.
- **IP address:** Displays the IP address of the selected device, or the management IP address for a device with multiple IP addresses.
- **Node Number:** Displays the node number assigned to the software or appliance node, between 1 and 120.
- **Customer ID:** Displays an optional user-defined ID. Customer IDs for in-line pairs and interface groups reflect the 7100 Series appliance nodes to which they belong.
- **Model:** Displays the model number of a 7100 Series appliance, either 7120, 7160, or 7161.
- **Monitoring Group:** Identifies the monitoring group of the selected device, if any.
- **Monitored Networks:** Identifies the networks for which port usage patterns are tracked and anomalies detected. Displayed only if you entered network IP addresses on the Network tab when editing interfaces, adding in-line pairs, or adding interface groups. Available only on 7100 Series interfaces.
- **TCP Reset Interface:** Displays the interface that sends TCP resets; either eth0, eth1, or eth2, corresponding to your choice of RST0, RST1, or RST2 when you added the interface group.
- **Bandwidth:** Displays the expected throughput for the selected object.

- **Sensor Status:** Displays the current status of the related sensor.
- **Description:** Displays a brief optional description of the object.
- **Active Security Incidents:** Displays the active incidents of the selected topology object, with name, state, node number, and last date modified.

Viewing objects in the topology tree

This section describes the following network elements represented on the topology tree in the Devices tab of Network Security:

- [About location objects](#)
- [About router objects](#)
- [About Symantec Network Security objects](#)
- [About Smart Agents](#)
- [Viewing the topology tree](#)
- [Viewing the topology tree](#)

Viewing auto-generated objects

The installation process automatically creates a number of objects in the topology tree. These objects can be renamed and configured, and in some cases, you can add more of them to the topology tree. For example, the installation process creates an object for one location in the topology tree, called Enterprise by default. Users can add more location objects to represent other locations. Symantec Network Security also automatically creates objects for managed network segments in the topology tree.

See the following for related information:

See [“About location objects”](#) on page 51.

See [“About managed network segments”](#) on page 62.

About location objects

The Symantec Network Security installation process automatically adds one location named Enterprise. A location object represents any physical or logical group of managed network segments. Each location must contain one or more network segments. A cluster of Symantec Network Security nodes can contain multiple locations, and you can add more objects to represent them. At least one location object must exist in the topology tree before you can add software or appliance nodes, device objects, or interface objects.

About Symantec Network Security objects

The installation process automatically creates an object in the topology tree to represent the first software or appliance node. This defaults to master node status, and the installation program automatically assigns it a node number of 1. By default, all software and appliance nodes installed in the network after this master node default to slave node status. The master node synchronizes the databases on all slave nodes in a cluster to its topology, detection and response policy, and configuration databases.

Under Enterprise, the location object created automatically during the installation process, SuperUsers can add objects to represent each Network Security software node and 7100 Series appliance node.

About software nodes

Software nodes are the objects that represent Symantec Network Security software installed on designated computers. Under Enterprise, the location object created automatically during the installation process, SuperUsers can add an object to the topology tree to represent each Network Security software node.

Viewing software nodes

The Devices tab displays detailed information about each object in the topology tree, upon selection. The Advanced Network Options tab contains information about the designated computer that this node represents in the topology tree. The installation process automatically provides this information.

Note: Both StandardUsers and RestrictedUsers can view software or appliance nodes, but cannot add, edit, or delete them.

To view software nodes

- 1 On the **Devices** tab, do one of the following:
 - Click an existing monitoring interface to view summary information in the right pane.
 - Right-click an existing software node, and click **Edit** to view detailed information.
- 2 In **Edit Software Node**, click the **Node Options** tab.
The following list describes the node option fields:
 - Name Indicates the descriptive name of the object, established when added to the topology tree.

- Customer ID Indicates an optional identification.
- IP Indicates the IP address for the node; administration IP address if the node is positioned behind a NAT device.
- Node Number Indicates the unique node number.
- Monitoring Group Indicates the monitoring group the node is assigned to, if any.
- Failover Group Indicates the failover group and identifying group number, if any.
- Master Node Sync Info Indicates the synchronization password and confirmation, if the node is part of a cluster.
- Description Includes any optional notes about the selected node.

3 In Edit Software Node, click the **Advanced Network Options** tab.
The following list describes the advanced network option fields:

- Local IP Indicates the internal IP address for a node behind a NAT router.
- Netmask Indicates which part of the node's IP address applies to the network.
- Default Router Indicates the IP address of the router that sends network traffic to and from the node.
- DNS Server 1 Indicates the primary Domain Name Service server for the node, which maps hostnames to IP addresses.
- DNS Server 2 Indicates the secondary Domain Name Service server for the node.
- Hostname Indicates the name of the host.

4 Click Cancel to close the view.

About monitoring interfaces

Monitoring interfaces communicate between the Symantec Network Security software or appliance node, and the network device, such as a router. The software or appliance node receives data about traffic on the router via the monitoring interface. SuperUsers can add objects to represent monitoring interfaces that connect software or appliance nodes to network devices.

Viewing monitoring interface objects

The Network Security console provides a way to view monitoring interfaces to the topology tree. The Interface and Networks tabs contain information about the designated computer that this node represents in the topology tree. The installation process automatically provides this information.

Note: Both StandardUsers and RestrictedUsers can view monitoring interfaces, but cannot add, edit, or delete them.

To view monitoring interfaces on software nodes

- On the **Devices** tab, do one of the following:
 - Click an existing monitoring interface to view summary information in the right pane.
 - Right-click an existing monitoring interface, and click **Edit** to view detailed information.
- In **Edit Monitoring Interfaces**, click the **Interface** tab.

The following list describes the interface fields:

■	Descriptive Name	Indicates the descriptive name of the object, established when added to the topology tree.
■	Interface Name	Indicates the name of the interface, established when added to the topology tree.
■	Customer ID	Indicates an optional identification.
■	Expected throughput	Indicates the expected throughput as established when added to the topology tree.
■	Description	Includes any optional notes about the selected node.
- In **Edit Monitoring Interfaces**, click the **Networks** tab to view the networks that this interface monitors.
- Click **Cancel** to close the view.

About appliance nodes

7100 Series appliance nodes are the objects that represent Symantec Network Security software installed on the new Symantec Network Security 7100 Series appliance.

Under Enterprise, the location object created automatically during the installation process, SuperUsers can add objects to represent each Symantec Network Security 7100 Series appliance node.

Viewing 7100 Series nodes

The Network Security console provides a way to view Symantec Network Security 7100 Series nodes. The installation process populates the fields in the Advanced Network Options tab blank. After installation, you can view the Advanced Network Options.

The Advanced Network Options tab contains information about the designated appliance that this node represents in the topology tree. The initial configuration process automatically provides this information. The fields remain blank until then.

Note: Both StandardUsers and RestrictedUsers can view software or appliance nodes, but cannot add, edit, or delete them.

To view 7100 Series nodes

- 1 On the **Devices** tab, do one of the following:
- Click an existing 7100 Series node to view summary information in the right pane.

■ Right-click an existing 7100 Series node, and click **Edit** to view detailed information.
- 2 In **Edit 7100 Series nodes**, in the **Node Options** tab, the following list describes the fields:
- Model

Indicates the model number of the 7100 Series node.

■ Name

Indicates the descriptive name of the object, established when added to the topology tree.

■ Customer ID

Indicates an optional identification.

■ IP

Indicates the IP address for the node; administration IP address if the node is positioned behind a NAT device.

■ Node Number

Indicates the unique node number.

■ Monitoring Group

Indicates the monitoring group the node is assigned to, if any.

■ Failover Group

Indicates the failover group and identifying group number, if any.

- Master Node Sync Info Indicates the synchronization password and confirmation, if the node is part of a cluster.
- Description Includes any optional notes about the selected node.

3 In **Edit 7100 Series Node**, click the **Advanced Network Options** tab.
The following list describes the advanced network option fields for a 7100 Series node:

- Local IP Indicates the internal IP address for a node behind a NAT router.
- Netmask Indicates which part of the node's IP address applies to the network. Required field.
- Default Router Indicates the IP address of the router that sends network traffic to and from the node. Required field.
- DNS Server 1 Indicates the primary Domain Name Service server for the node, which maps hostnames to IP addresses.
- DNS Server 2 Indicates the secondary Domain Name Service server for the node.
- Hostname Indicates the hostname of the 7100 Series node.

4 Click **Cancel** to close the view.

About 7100 Series interfaces

Each Symantec Network Security 7100 Series interface is a point of contact between the 7100 Series node and a network device. The node accesses traffic on the network device via the interface.

There are three interface types available on a 7100 Series node:

- Monitoring interface A single interface that monitors network traffic copied to it from a network device. Also known as a passive mode interface. Monitoring interface objects are automatically generated when a node object is added.
- Interface group Two to four passive mode interfaces sharing a single sensor. Used in an asymmetrically routed environment.
- In-line pair Two interfaces cabled into the actual network traffic path, and configured for in-line mode. Allows blocking of malicious traffic.

Viewing a monitoring interface on a 7100 Series node

The Network Security console provides a way to view the automatically generated interface objects on a 7100 Series node.

Note: Both StandardUsers and RestrictedUsers can view monitoring interfaces, but cannot add, edit, or delete them.

To view monitoring interfaces on 7100 Series nodes

- 1 On the **Devices** tab, do one of the following:
 - Click an existing monitoring interface to view summary information in the right pane.
 - Right-click an existing monitoring interface, and click **Edit** to view detailed information.
- 2 In **Edit Monitoring Interfaces**, click the **Interface** tab.
 The following list describes the interface fields:

■	Descriptive Name	Indicates the descriptive name of the object, established when added to the topology tree.
■	Interface Name	Indicates the name of the interface, established when added to the topology tree.
■	Customer ID	Indicates an optional identification.
■	Expected throughput	Indicates the expected throughput as established when added to the topology tree.
■	TCP Reset Interface	Indicates the interface to TCP resets.
■	Description	Includes any optional notes about the selected node.
- 3 In **Edit Monitoring Interfaces**, click the **Networks** tab to view the networks that this interface monitors.
- 4 Click **Cancel** to close the view.

Viewing interface groups

The Network Security console provides a way to view interface group objects on a 7100 Series node.

To view an interface group

- 1 On the **Devices** tab, do one of the following:

- Click an existing interface group to view summary information in the right pane.
 - Right-click an existing interface group, and click **Edit** to view detailed information.
- 2 In **Edit Interface Group**, in the **Interface Group** tab.
- The following list describes the interface fields:
- Name Indicates the descriptive name of the object, established when added to the topology tree.
 - Expected throughput Indicates the expected throughput as established when added to the topology tree.
 - TCP Reset Interface Indicates the interface to TCP resets.
 - Description Includes any optional notes about the selected node.
- 3 In **Edit Interface Group**, click the **Networks** tab to view the networks that this interface monitors.
- 4 In **Edit Interface Group**, click the **Interface** tab to view the interfaces that belong to this group.
- 5 Click **Cancel** to close the view.

Viewing in-line pairs

The Network Security console provides a way to view in-line pairs on a 7100 Series node.

To view an in-line pair

- 1 On the **Devices** tab, do one of the following:
- Click an existing in-line pair to view summary information in the right pane.
 - Right-click an existing in-line pair, and click **Edit** to view detailed information.
- 2 In **Edit In-line Pair**, in the **In-line Pair** tab, view the following information:
- Name Indicates the descriptive name of the object, established when added to the topology tree.
 - Expected throughput Indicates the expected throughput as established when added to the topology tree.
 - Pair Indicates the interfaces included in the pair.

- **Description** Includes any optional notes about the selected node.
- 3 In **Edit In-line Pair**, click the **Networks** tab to view the networks that this interface monitors.
 - 4 In **Edit In-line Pair**, click the **Interface** tab to view the interfaces that belong to this group.
 - 5 Click **Cancel** to close the view.

About router objects

Routers store data packets and forward them along the most expedient route between hosts or networks. Symantec Network Security monitors this connection. Add an object to the topology tree to represent each router that you want Symantec Network Security to monitor.

Viewing router objects

The Network Security console provides a way to view routers.

To view a router object

- 1 On the **Devices** tab, do one of the following:
 - Click an existing router object to view summary information in the right pane.
 - Right-click an existing router object, and click **Edit** to view detailed information.
- 2 In **Edit Router**, the following list describes the information fields:
 - **Name** Indicates the descriptive name of the object, established when added to the topology tree.
 - **Customer ID** Indicates optional unique identification.
 - **IP** Indicates the IP address.
 - **SNMP** Indicates the optional SNMP password and confirmation, if any.
 - **Description** Includes any optional notes about the selected node.
- 3 Click **Cancel** to close the view.

About router interfaces

An interface object represents each router interface through which Symantec Network Security tracks attacks.

To view a router interface

- 1 On the **Devices** tab, do one of the following:
 - Click an existing router interface to view summary information in the right pane.
 - Right-click an existing router interface, and click **Edit** to view detailed information.
- 2 In **Edit Router Interface**, the following information is displayed:

■ Name	Indicates the descriptive name of the object, established when added to the topology tree.
■ Interface Name	Indicates the name of the selected interface according to the manufacturer's naming conventions.
■ Customer ID	Indicates an optional unique identification.
■ IP	Indicates the IP address for the interface.
■ Netmask	Indicates the netmask for the interface.
■ Description	Includes any optional notes about the selected node.
- 3 Click **Cancel** to close the view.

About Smart Agents

Symantec Network Security Smart Agents are translation software that enable Symantec Network Security to receive event data from external sensors, and correlate that data with all other events.

Smart Agents expand the security umbrella and enhance the threat detection value of existing security assets by aggregating third-party intrusion events into Symantec Network Security, which leverages its correlation, analysis, and response functionality.

Symantec Network Security contains an internal Smart Agent configuration to integrate Symantec Decoy Server events. To integrate events from any other external sensor, you must install an external Smart Agent designed for that sensor, and add a Smart Agent object to the topology tree to represent it.

To view a Smart Agent

- 1 On the **Devices** tab, do one of the following:
 - Click an existing Smart Agent object to view summary information in the right pane.
 - Right-click an existing Smart Agent object, and click **Edit** to view detailed information.
- 2 In **Edit Smart Agent**, the following information is displayed:

■ Name	Indicates the descriptive name of the object, established when added to the topology tree.
■ Customer ID	Indicates an optional unique identification.
■ IP	Indicates the IP address for the Smart Agent.
■ Type	Indicates the type of external sensor.
■ Receiver	Indicates the node that will receive data from an external sensor.
■ EDP Password	Indicates the EDP password and confirmation.
■ Description	Includes any optional notes about the selected node.
- 3 Click **Cancel** to close the view.

About Smart Agent interfaces

Smart Agent interface objects serve as a visual reminder of the location of any Symantec Network Security Smart Agents in the network. They also make Symantec Network Security aware for the TrackBack response action.

To view Smart Agent interfaces

- 1 On the **Devices** tab, do one of the following:
 - Click an existing Smart Agent interface to view summary information in the right pane.
 - Right-click an existing Smart Agent interface, and click **Edit** to view detailed information.
- 2 In **Edit Smart Agent**, the following information is displayed:

■ Name	Indicates the descriptive name of the object, established when added to the topology tree.
■ Customer ID	Indicates an optional unique identification.

- IP Indicates the IP address for the Smart Agent.
- Netmask Indicates the netmask.
- Description Includes any optional notes about the selected node.

3 Click **Cancel** to close the view.

About managed network segments

Managed network segments include each unique subnet in which the network devices and interfaces reside. The Network Security console automatically creates an object in the topology tree to represent each such managed network segment in your network. Each time you add a new interface object, Symantec Network Security adds a new object for the network segment in which the interface resides, if not already represented. SuperUsers can edit the default name (**Untitled**) and the description.

Symantec Network Security automatically creates a managed network segment object for each unique subnet in which the network devices and interfaces reside. When a new interface object is created, Network Security adds a new object for the network segment in which the interface resides, if that segment has not already been represented by an object.

To view network segments

- 1 On the **Devices** tab, do one of the following:
 - Click an existing network segment object to view summary information in the right pane.
 - Right-click an existing network segment object, and click **Edit** to view detailed information.
- 2 In **Edit Network Segment**, the following information is displayed:
 - Name Indicates the descriptive name of the object, established when added to the topology tree.
 - Network Indicates the selected network.
 - Netmask Indicates the netmask.
 - Description Includes any optional notes about the selected node.
- 3 Click **Cancel** to close the view.

Launching Symantec Decoy Server

Now you can launch and log into the Symantec Decoy Server console by simply right-clicking any external sensor object in the topology tree and selecting **Start Decoy Console**. Note that the Symantec Decoy Server console remains open, even if you close the Network Security console.

This section includes the following:

- [Launching from a new location](#)
- [Launching from a known location](#)

Launching from a new location

This section describes how to launch the Symantec Decoy Server console from a new location on the network.

To launch the Symantec Decoy Server console from a new location

- 1 Right-click any external sensor object in the topology tree, and click **Start Decoy Console**.
- 2 The first time, a **Decoy Console Not Found** message appears. Click **OK**.
- 3 In **Select the Symantec Decoy Server Console Directory**, navigate to the directory containing `mtadmin.jar`, and click **Open**.
This file is typically located in `Program Files\Symantec\Mantrap`.
- 4 In **Start Decoy Console**, click **Yes** to confirm the path to the jar file.
After launching the Symantec Decoy Server console from this new location, the location of the `mtadmin.jar` file is stored in memory.

Launching from a known location

This section describes how to launch the Symantec Decoy Server console from a known location on the network.

To launch the Symantec Decoy Server console from a known location

- 1 Right-click any external sensor object in the topology tree, and click **Start Decoy Console**.
- 2 In **Start Decoy Console**, click **Yes** to confirm the path to the `mtadmin.jar` file.

Note: The Symantec Decoy Server console must be closed independently of the Network Security console. The Symantec Decoy Server console remains open, even if you close the Network Security console.

Protection Policies

This chapter includes the following topics:

- [About protection policies](#)
- [Viewing protection policies](#)
- [Adjusting the view of event types](#)

About protection policies

Symantec Network Security provides a new functionality called protection policies, which utilize multiple components such as signature and protocol anomaly detection to take action directly at the point of entry into the network. Protection policies enable users to tailor the protection based on security policies and business need. Policies can be tuned by threat category, severity, intent, reliability, and profile of protected resources. Common or individualized policies can be applied per sensor, for both in-line and passive monitoring.

The Symantec Network Security software and the Symantec Network Security 7100 Series appliance employ a common core architecture that provides detection, analysis, storage, and response functionality. Most procedures in this section apply to both the 7100 Series appliance and the Symantec Network Security 4.0 software. The 7100 Series appliance also provides additional functionality that is unique to an appliance. Each section describes this additional functionality in detail.

For example, when the 7100 Series appliance is deployed in-line, it can perform session-based blocking against malicious traffic and prevent attacks from reaching their targets.

Viewing protection policies

Symantec Network Security provides a set of pre-defined protection policies that include attack policies, audit policies, and prevention policies. They can be immediately activated by setting them to interfaces and applying them. You can also define your own policies and activate them using the same procedures.

On the Protection Policies tab, you can view all available protection policies in the left pane, and the node interfaces that they are applied to, in the right pane.

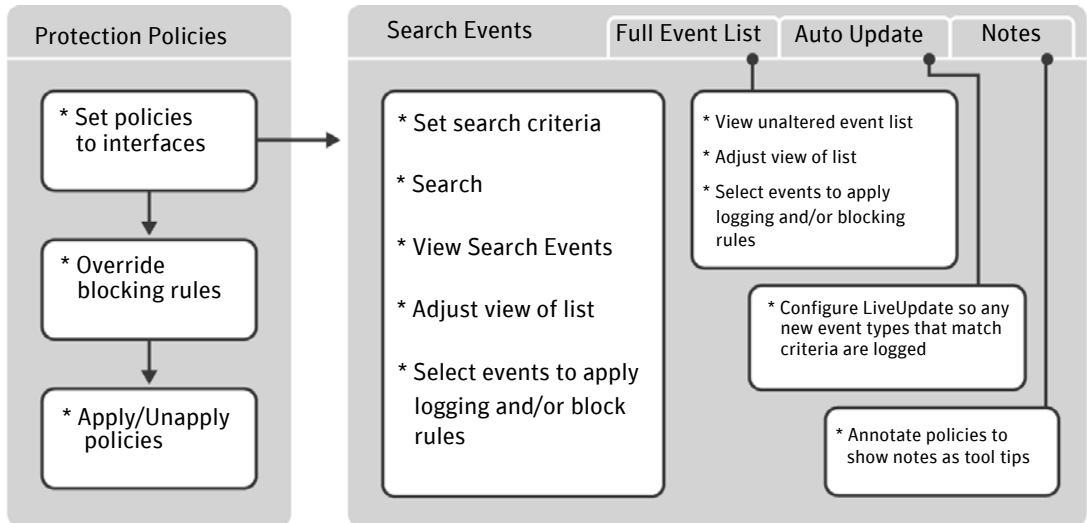


To see all available protection policies and interfaces

- 1 On the **Policies** tab, click **Protection Policies**.
- 2 Select an existing policy, and click **View**.

Understanding the protection policy view

The Protection Policies view contains five main tabs, as follows:



The following list describes each tab more fully:

- **Protection Policies tab:** Symantec Network Security installs with a set of pre-defined policies that you can use immediately by setting them to interfaces, override existing blocking rules, and applying them.
 - [Viewing protection policies](#)
- **Search Events tab:** At first, the Search Events tab displays the full list of event types that the selected policy can detect. You can reduce this list to a more manageable size by setting search parameters. Then the Search Results pane displays a subset of the types of events that you specified. You can apply logging and/or blocking rules from this tab, and add new protection policies that you define yourself.
 - [Adjusting the view by searching](#)
- **Full Event List tab:** The Full Event List displays all event types that the selected policy can detect. Even after you define the display on the Search Events tab, you can use the Full Event List to view the total list of all event types. You can also set logging and blocking rules from this tab.
- **Auto Update tab:** Provides the ability to establish automatic policy, signature, and engine updates through LiveUpdate.
 - [Viewing policy automatic update](#)

- *Notes tab*: Provides the ability to annotate policies so that your note is displayed as a tool tip when you hover the cursor over the annotated policy.
 - [Annotating policies or events](#)

Adjusting the view of event types

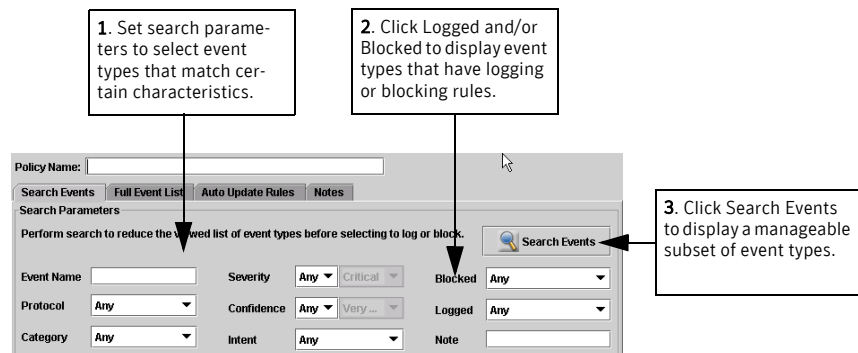
You can adjust the view of the event types list by using the Search Events tab. You can also select which columns to show or hide, and sort the column data.

This section describes the following topics:

- [Adjusting the view by searching](#)
- [Adjusting the view by columns](#)
- [Viewing event detailed descriptions](#)

Adjusting the view by searching

Symantec Network Security provides search functionality so that you can focus the view on a manageable subset of possible event types with specific characteristics. The policy still detects and acts on the full list of event types; but you have a shorter list to sift through as you decide what to block and what to log. This section describes how to narrow or widen the view by searching for event types that match certain characteristics.



To adjust the view by searching for specific characteristics

- 1 In the **Policies** tab, do one of the following:
 - Select a policy, and click **View > Search Events**.
- 2 Provide some or all of the following search criteria:
 - In **Event Name**, enter a name.
 - In **Protocol**, select a protocol from the pull-down list.

- In **Category**, select a category from the pull-down list.
 - In **Severity**, set a severity level from the pull-down list.
 - In **Confidence**, set a confidence level from the pull-down list.
 - In **Intent**, select an intention from the pull-down list.
 - In **Blocked**, specify whether you want to view events with blocking rules.
 - In **Logged**, specify whether you want to view events with logging rules.
 - In **Note**, specify the contents of the Note to search for events containing the specified contents.
- 3 Click **Search Events**.
Search Results displays the total number of items shown in the subset.
 - 4 Click **OK** to save and exit.

Note: Remember that the policy still contains the full list of event types. This search has provided a shorter, more manageable subset to view.

Note: Both StandardUsers and RestrictedUsers can adjust the view of event types in a policy by searching for a subset of the list.

Adjusting the view by columns

Both the Search Events and Full Event List provide the ability to adjust the display by selecting, moving, and sorting columns.

To adjust the view of both full and search events

- 1 In the **Policies** tab, do one of the following:
 - Click **New**.
 - Select a protection policy, and click **View**.
- 2 Do one of the following:
 - Click **Search Events**.
 - Click **Full Event List**.
- 3 Click **Columns**.
- 4 In **Table Column Chooser**, click each column that you want to see, and unclick each that you want to hide.
- 5 Click a column heading to sort the table by one level.
- 6 Click **OK**.

Note: Both StandardUsers and Restricted Users can adjust the view of events in protection policies by showing and hiding columns.

Viewing logging and blocking rule details

Symantec Network Security provides a view of the logging and blocking rules applied to each event type in a policy.

To view individual protection policies

- 1 On the **Policies** tab, select a protection policy.
- 2 Click **View**.
- 3 In **Full Event List**, select an event type, and clicking **Log/Block**.
- 4 Click **Cancel** to exit.

Note: StandardUsers can view event details; RestrictedUsers cannot.

Viewing event detailed descriptions

Symantec Network Security provides detailed descriptions of the event types in each policy through a browser display.

To view individual protection policies

- 1 On the **Policies** tab, select a protection policy.
- 2 Click **View**.
- 3 In **Full Event List**, right-click an event type
- 4 Click **View Description** to display a detailed description in your browser.
- 5 Click **Cancel** to exit.

Note: StandardUsers can view event details; RestrictedUsers cannot.

Viewing policy automatic update

The LiveUpdate functionality puts newly developed signatures to work immediately by applying four criteria (category, protocol, severity, and confidence). When LiveUpdate downloads new signatures into your system, Auto Update Rules selects those signatures that match the criteria, and

automatically adds them to the policy. Even if the LiveUpdate occurs in the middle of the night, Symantec Network Security immediately starts logging the matching events.

To view LiveUpdate

- 1 In the **Policies** tab, click **Protection Policies > View > Auto Update Rules**.
- 2 Click **Cancel** to close the view.

Note: Both StandardUsers and RestrictedUsers can view Auto Update rules, but cannot add, edit, or delete them.

Annotating policies or events

You can take notes on events at the following three levels:

- [Viewing policy annotations](#)
- [Viewing event type annotations](#)
- [Annotating event instances](#)

Viewing policy annotations

If notes were taken about a particular policy, then when you hover the cursor over that policy in the policy list, the note appears as a tool tip.

To view a policy annotation

- ◆ In the **Policies** tab, hover the cursor over the policy to display the note as a tool tip.

Note: Both StandardUsers and RestrictedUsers can view tool tips to protection policies, but cannot add, edit, or delete them.

Viewing event type annotations

The Network Security console provides a field in which to make notes about an event type within a policy. When the event is triggered, the note is displayed in the Event Details. For example, a note might indicate that this event is a false positive if it occurs within a certain IP range. The note is specific to that event type when it occurs in that policy. The Event Details pane displays the note each time this policy detects the annotated event.

To view notes about an event types in a policy

- 1 In the **Policies** tab, click **View**.
- 2 In **View Protection Policy**, do one of the following:
 - In **Search Events**, double-click an event.
 - In **Full Event List**, double-click an event.
- 3 In **Note for Selected Event Type(s)** in the lower pane, view the annotation about the selected event type.
- 4 Click **Cancel** to close the view.

Note: Both StandardUsers and RestrictedUsers can view notes to event types, but cannot add, edit, or delete them.

Annotating event instances

The Network Security console provides a field in which to make notes about a specific instance of an event. This provides assistance to system analysts in resolving security incidents.

To view note about an instance of an event

- 1 In the **Incidents** tab, do one of the following:
 - Double-click an incident.
 - In the upper pane, click an incident, and then in the lower pane, double-click the related event.
- 2 In **Incident Details** or **Event Details**, click **Analyst Note**.
- 3 Enter your annotation, and click **Add Note**.
- 4 Click **Close**.

Note: Both StandardUsers and RestrictedUsers can add notes to instances of an event.

Response Rules

This chapter includes the following topics:

- [About response rules](#)
- [About automated responses](#)
- [Viewing response rules](#)
- [About response parameters](#)
- [About response actions](#)
- [About flow alert rules](#)

About response rules

In addition to the ability to start detection and response immediately using protection policies, Symantec Network Security also provides an automated, rule-based response system. The response module responds to incidents immediately, even if you cannot maintain system analysts on site around the clock. The response module identifies, prioritizes, and responds appropriately to whole classes of attacks, without requiring a separate response rule for each of hundreds of individual base events. SuperUsers and Administrators can create separate response rules specific to an individual event type, to any subset of specified event types, or to all event types. This affords fast, effective responses to suspicious behavior, and enables you to move quickly to stop attacks, even DoS attacks, to mitigate potential damage, lost revenue, and the costs of recovery.

The Symantec Network Security software and the Symantec Network Security 7100 Series appliance employ a common core architecture that provides detection, analysis, storage, and response functionality. Most procedures in this section apply to both the 7100 Series appliance and the Symantec Network Security 4.0 software. The 7100 Series appliance also provides additional

functionality that is unique to an appliance. Each section describes this additional functionality in detail.

Symantec Network Security can take the following types of actions to respond to attacks, individually or in sequence:

- Predefined actions
See [“About response actions”](#) on page 79.
- Configured custom response actions
See [“About custom response action”](#) on page 81.
- Triggered actions from third-party applications via Smart Agents
See [“Integrating third-party events”](#) on page 282.
- No actions
See [“About no response action”](#) on page 80.
- Responding at the point of entry
See [“Defining new protection policies”](#) on page 120.

About automated responses

Symantec Network Security’s automated rule-based response system includes alerting, pinpoint traffic recording, flow tracing, session resetting, and custom responses on both the software and appliance nodes and the Network Security console. Symantec Network Security generates responses based on multiple criteria such as event targets, attack types or categories, event sources, and severity or confidence levels. Multiple responses can be configured for the same event type, as well as the order in which Symantec Network Security executes the responses.

Symantec Network Security reviews each event, and iterates through the list of response rules configured by the user. It compares each event against configurable match parameters. If a match occurs on all parameters, it then executes the specified action. After Symantec Network Security processes one rule, it proceeds to one of three alternatives: to the rule indicated by the Next parameter, to a following rule beyond the Next rule, or it stops policy application altogether for this event.

Some automated responses also use node parameters through Configuration > Node > Network Security Parameters. Symantec Network Security installs with some of the response rule parameters defaulted; however, they require more information to run successfully.

Note: Both StandardUsers and RestrictedUsers can view response rules, but cannot configure, edit, or delete them.

Viewing response rules

All users can view the response rules in the Network Security console.

To view Response Rules

- In the Network Security console, click **Configuration > Response Rules**.
- In **Response Rules**, select a response rule. The background of the selected response rule turns purple.
- Click a column to view the following response parameters:
 - Event Target
 - Event Type
 - Severity
 - Confidence
 - Event Source
 - Response Action
 - Next Action
- Click the **Response Actions** column of a response rule to see all possible response actions.

Interpreting color coding

At a glance, you can tell which response rules have been saved, and which remain to be saved, by the background colors:

Color	Indication
White	Indicates the response rule has been saved
Yellow	Indicates the response rule has not been saved
Purple	Indicates the response rule is currently selected

Select an entire row by clicking the number cell.

Note: Make sure to click **OK** to save yellow response rules before proceeding.

Searching event types

All users can view a more manageable subset of the entire event list by using any or all of the search criteria to shorten the list of event types in the Search Event List.

To select event types

- 1 In the Network Security console, click **Configuration > Response Rules > Event Type**.
- 2 To see the Event Lists, double-click **Event Types**.
- 3 In **Search Events**, provide some or all of the following search criteria:
 - Click **Title** to identify the search.
 - Click **Protocol** to search for specific protocols.
 - Click **Category** to search for specific categories.
 - Click **Severity** to indicate the severity level.
 - Click **Confidence** to indicate the confidence level.
 - Click **Intent** to indicate the intent.
- 4 After selecting search criteria, click **Search Events**.

About response parameters

In Configuration > Response Rules, SuperUsers and Administrators can edit and configure response rule parameters to specify the characteristics of the events and incidents that Symantec Network Security responds to.

Each response rule contains the following response parameters:

- [About event targets](#)
- [About event types](#)
- [About severity levels](#)
- [About confidence levels](#)
- [About event sources](#)
- [About response actions](#)
- [About next actions](#)

About event targets

The event target parameter specifies the location where the detected incident occurs. The possible values for this parameter include the locations, network

segments, and network border interfaces defined in the network topology database.

About event types

The event type parameter specifies the base event or events for which the response rule is defined. Event types are grouped into several larger protocol and service attack categories. When Symantec Network Security detects a suspicious event, it analyzes the event to match it to an event type.

About severity levels

The severity parameter describes the relationship between the action to take in response to an incident and the severity of that incident. Before the analysis process assigns a severity level to an incident, it analyzes the various events that make up the incident according to the following factors:

- **Intrinsic severity of the type of event:** An event might consist of an FTP packet transmitted on port 80. Because port 80 is used for HTTP traffic, this event might represent an attack on a Web server. By itself, this example might represent a medium level of intrinsic severity.
- **Level of traffic, if it is a counter event:** If Symantec Network Security determines that a series of packets make up a flood attack, the height of the severity level depends on the number and frequency of packets received.
- **Severity of other events in the same incident:** Symantec Network Security correlates severity levels from all events in the same incident.

By using these variables to perform statistical analysis, Symantec Network Security assigns different severity levels as they apply to an incident. As the system gains information about the network, it integrates characteristics that influence the levels to reflect the current state of the network security.

Because the traffic on every network is different, the severity levels specified in the response rule parameters are relative values and contain no inherent absolute definition. The creation of response rules in general and the selection of severity levels for the specific response rules requires fine-tuning to existing security response rules, as well as to the network traffic and ambient conditions.

If the severity assigned during analysis equals the severity level defined in the response rule, as well as all other parameters defined in the response rule, then Symantec Network Security responds to the incident by performing the action associated with the response rule. SuperUsers and Administrators can also specify that the action execute only if the incident priority level falls above or below that of a particular severity level. Possible severity parameter values include informational, low, medium, high, and critical.

About confidence levels

Symantec Network Security indicates the confidence level, a measure of the likelihood of an actual attack. It determines the confidence level of the event by analyzing the traffic behavior.

About event sources

The Network Security console can apply response rules to specific locations or interfaces in the network using Event Source. The event source parameter indicates that a rule applies only to events detected on a given interface. This interface is not necessarily the target of the attack, but may in fact be the point in the network at which Symantec Network Security is currently tracking the attack. If the interfaces being inspected are receiving VLAN encapsulated traffic, you can also specify that a rule applies to a specific VLAN ID.

About response actions

The Network Security console provides a way to apply the response rule to take a specific action when triggered using Response Action. The Response parameter determines the action Symantec Network Security takes if an incident matches the event target, attack type, severity, confidence level, and event source parameters. SuperUsers and Administrators can set multiple response actions to react to specific types of incidents, or set custom response actions to launch third-party applications in response to an incident.

Note: StandardUsers and RestrictedUsers can view response rules, but cannot apply, edit, or delete them.

Symantec Network Security can take the following action or sequence of actions in response to an event that matches the criteria:

- [About no response action](#)
- [About email notification](#)
- [About SNMP notification](#)
- [About TrackBack response action](#)
- [About custom response action](#)
- [About TCP reset response action](#)
- [About traffic record response action](#)
- [About console response action](#)

- [About export flow response action](#)

About next actions

The Network Security console provides a way to direct a sequence of response rules that conclude with a follow-up action by using Next Action.

The Next parameter determines whether or not Symantec Network Security continues checking for additional response rules that match the incident. Possible values are Stop, Continue to Next Rule, and Jump to Rule. The Continue to Next Rule value directs Symantec Network Security to search for the next matching response rule after executing the current response rule. This enables Symantec Network Security to make multiple responses to any particular incident type, in combination with each other and in a desired sequence. The Jump to Rule value directs Symantec Network Security to skip over intervening response rules and go directly to a particular response rule, such as from Rule 5 to Rule 8. The Stop value directs Symantec Network Security to discontinue searching for matching response rules.

About response actions

Configurable response parameters indicate which action Symantec Network Security will take if the event target, attack type, severity, confidence level, and event source parameters match the incident. The SuperUser or Administrator can define and customize response actions from the Network Security console. If you specify a Smart Agent response action, the policy manager sends the respective values to the appropriate Smart Agent. In Configuration > Response Rules, select a rule, and click the Response Actions column to view the list of actions that Symantec Network Security can take in response to an incident.

Symantec Network Security can respond to an incident via the following response actions:

- [About no response action](#)
- [About email notification](#)
- [About SNMP notification](#)
- [About TrackBack response action](#)
- [About custom response action](#)
- [About TCP reset response action](#)
- [About traffic record response action](#)
- [About console response action](#)

- [About export flow response action](#)

About no response action

The **None** option directs Symantec Network Security not to respond to particular types of incidents. Selecting the None option, followed by Stop as the next action configures Symantec Network Security to take no action in response to specified types of incidents. SuperUsers and Administrators can also configure Symantec Network Security to ignore specific attacks by setting a filter.

About email notification

Alerting is a standard component of most intrusion detection systems because security analysts must be kept informed of attack activity without having to constantly monitor the Network Security console. Unfortunately, many IDS products use the same interface for detection as for notification. In such a configuration, a flood attack could prevent the console from sending email notifications because the flood attack would overload the interface.

Symantec Network Security uses a separate, independent interface for notification, thus enabling the Network Security console to successfully send email notification even during an attack.

About SNMP notification

Symantec Network Security can initiate an SNMP notification in response to an attack. The SNMP notification option directs Symantec Network Security to send SNMP traps to an SNMP manager with a minimum delay of 1 minute between responses. The IP address of the SNMP manager must be provided, and the SNMP manager made aware of the Management Information Base (MIB). Refer to the SNMP manager documentation for this information.

About TrackBack response action

Symantec Network Security provides the TrackBack™ response to track attacks back to their sources. This capability is especially important for tracking denial-of-service attacks that must be traced to their source in order to shut them down most effectively. TrackBack automatically tracks a data stream to its source within the cluster, or, if the source is outside the cluster, to its entry point into the cluster. It does this by gathering information from routers or its own sensor resources. Sensors require interfaces with applied protection policies to run, as well as sensor parameters for flow statistics.

About custom response action

The Network Security console provides a way to set custom response actions to launch third-party applications in response to an incident. To do this, a command is entered in the Custom Response field which executes when the response rule is triggered. The minimum delay between responses is 0.

Note: Both StandardUsers and RestrictedUsers can view custom response actions, but cannot write them.

About TCP reset response action

The TCP reset response action directs Symantec Network Security to terminate a TCP connection to prevent further damage from an attack. The minimum delay between responses is 0.

About traffic record response action

The traffic record response dynamically records network traffic in response to an event. With this option, Symantec Network Security can record traffic for a specified period of time, or until a specified number of packets has been collected.

The traffic record response action begins recording traffic when triggered. It continues to record based on the number of minutes and the number of packets specified in the response configuration. Traffic recording stops when either limit is reached, whichever comes first. If the maximum number of packets is reached before the maximum time, then traffic record stops recording, but waits until the maximum time has expired before starting a new record action. The number of responses per incident is also determined by the response configuration. The minimum delay between responses is 1 minute.

The traffic record response action begins recording traffic when triggered. It continues to record based on the number of minutes and the number of packets specified in the response configuration. Traffic recording stops when either limit is reached, whichever comes first. If the maximum number of packets is reached before the maximum time, then traffic record stops recording, but waits until the maximum time has expired before starting a new record action. The number of responses per incident is also determined by the response configuration. The minimum delay between responses is 1 minute.

Note: This response action records only fully assembled packets from actual flows, not malformed packets or packet fragments. You can view detected packet contents in the Advanced tab of Event Details.

See [“Viewing event details”](#) on page 197.

About console response action

Symantec Network Security can initiate an action on the Network Security console in response to an attack. A SuperUser or Administrator can configure the response rule to play an alert sound and/or to execute a program on the Network Security console. Any user can enable each Network Security console individually to execute console response actions. The minimum delay between responses is 1 minute.

Enabling console response actions

You must enable console response actions on each Network Security console individually.

To enable specific console response actions

- 1 In the Network Security console, click **Configuration > Response Rules**.
- 2 In **Response Rules**, click **Configuration > Console Response Configuration**.
- 3 In **Local Console Configuration**, choose from the following checkboxes:
 - **Play Alert Sounds:** Click this to enable this Network Security console to emit an alert sound when triggered by an event.
 - **Execute Programs:** Click this to enable this Network Security console to perform the console response action.
- 4 In **Local Console Configuration**, click **OK** to save and close.

Note: The Network Security console must be running in order for Symantec Network Security to execute the console response action. If a Network Security console starts after console response events are sent, it does not execute the actions. Instead, upon startup, it displays a prompt indicating that the actions did not execute.

About export flow response action

The export flow response action exports matching flows stored in the flow data store. The action is based on the characteristics of the triggering events, which

are specified by parameters that the SuperUser provides when creating the rule. The SuperUser or Administrator can use Export Flow to specify the event characteristics of the triggering event. Flows that match the specified characteristics are exported and saved. The minimum delay between responses is 1 minute.

About flow alert rules

In addition to response rules, Symantec Network Security can respond to network traffic according to flow alert rules. Flow alert rules respond to traffic flows that violate defined policies on monitored networks. Flow alert rules can be configured to notify you when a sensor or router detects flows that match specific criteria.

Symantec Network Security collects data about network flows from various devices. It optimizes the data to enable advanced response actions such as TrackBack, and notifies you about illegal flows. Symantec Network Security uses FlowChaser to store the data, in coordination with TrackBack, which traces a DoS attack or network flow back to its source, or to the edges of the administrative domain.

Note: StandardUsers can view flow alert rules; and RestrictedUsers have no access at all.

Viewing flow alert rules

Symantec Network Security provides a way to view flow alert rules from the Network Security console.

To view flow alert rules

- ◆ In the Network Security console, click **Configuration > Flow Alert Rules**. In **Flow Alert Rule**, you can view the rule details.

Playing recorded traffic

Like the FlowChaser, Query Current Flows, and Query Exported Flows, the Traffic Playback Tool provides another way to search recorded data outside of the Network Security reporting system. When you set a response rule to record events of a particular description, you can then use the Traffic Playback Tool to replay and scrutinize the records of those events.

See [“Managing response rules”](#) on page 132.

Replaying recorded traffic flow data

The Network Security console provides a way to review recorded traffic data in two ways: from the **Query** button or from the **Incidents** tab on the main menu of the Network Security console. The record of events is displayed as a table with each row corresponding to one event. By selecting an event, you can display the flow or delete the event. In the flow view, you can replay the details of the traffic flow data.

To replay traffic flow data

- 1 Choose one of the following:
 - Click **Flows > Traffic Playback > select a node > OK**.
 - Click **Incidents > double-click the Traffic Record Finished event > Event Message**.
Skip Steps 2 and 3, and proceed directly to Step 4.
- 2 In **Traffic Playback Configuration**, you can adjust the view as follows:
 - To adjust your view of **Recorded Events**, click **Column**.
 - To remove events you do not want to view, click the event, and then click **Delete**.
- 3 In **Recorded Events**, click the row corresponding to an event to view the flow of that event in **Flows of Selected Record**.
- 4 In **Flows of Selected Record**, click a row corresponding to a flow, then click **Playback**.
- 5 In **Packet Replay Tool**, view the detailed packet data, one packet at a time.
- 6 To view all packet data in a session that includes multiple packets, on **Symantec Packet Replay Tool**, click **View > Show Session Window**.
- 7 Return to **Symantec Packet Replay Tool**, and click **Go**.

Note: SuperUsers can view playbacks of recorded traffic; Administrators, StandardUsers, and RestrictedUsers cannot. See “[User groups reference](#)” on page 319 for more about permissions.

Detection Methods

This chapter includes the following topics:

- [About detection](#)
- [About sensor detection](#)
- [About port mapping](#)
- [About signature detection](#)
- [About refinement rules](#)

About detection

In addition to the ability to start detection immediately using protection policies, Symantec Network Security also provides the tools to fine-tune the detection to a particular environment using sensor parameters and port mappings, and to enhance the detection using user-defined signatures. Symantec Network Security can run multiple detection methods concurrently, including protocol anomaly detection, signatures, IP traffic rate monitoring, IDS evasion detection, and IP fragment reassembly.

The Symantec Network Security software and the Symantec Network Security 7100 Series appliance employ a common core architecture that provides detection, analysis, storage, and response functionality. Most procedures in this section apply to both the 7100 Series appliance and the Symantec Network Security 4.0 software. The 7100 Series appliance also provides additional functionality that is unique to an appliance. Each section describes this additional functionality in detail.

■ Protocol anomaly detection

Symantec Network Security provides a way to tune the sensors to look for particular types of anomalies and signatures on a port by reconfiguring the default port mapping, or adding new mappings. For example, mappings can be

added to run services on non-standard ports or to ignore ports on which you normally run non-standard protocols, to mitigate common violations of protocol from being falsely reported as events.

■ Signature detection

Symantec Network Security provides the functionality to begin detection immediately by applying protection policies. In addition to this initial ability, detection can also be enhanced and tuned to a particular network environment by creating and applying user-defined signatures.

■ Refinement rule detection

Symantec Network Security detects both known and unknown (zero-day) attacks, using multiple detection technologies concurrently. Event refinement rules extend the Protocol Anomaly Detection capabilities. Symantec Network Security matches generic anomalies against a database of refinement rules, and for known attacks, reclassifies an anomaly event by retagging it with its specific name.

New refinement rules are available as part of SecurityUpdates on a periodic basis. Each software or appliance node downloads the refinement rules from LiveUpdate and stores them individually.

About sensor detection

Symantec Network Security provides an array of sensor parameters that are preset for optimum performance and sensitivity. They can be tuned to address specific network environments, and each sensor can be set individually to devote it to specific tasks. These parameters perform multiple tasks, such as enabling the collection of flow statistics and full packet data, setting threshold levels for floods, scans, and sweeps, and regulating the percentage of traffic types that the sensor tolerates before it notifies you.

The parameters also provide counter-based detection of floods and denial-of-service attacks such as resource reservation and pipe filling, regulate the suppression of duplicate events and enabling asymmetric routing, and enable checksum validation for a variety of traffic types.

Viewing sensor parameters

The Network Security console provides a way to view descriptions of sensor parameters. The upper right pane of the Sensor Parameters dialog displays a description of the parameter. The lower right pane displays the current value.

To view the sensor parameters

- 1 On the **Devices** tab, right-click the sensor.
- 2 Click **Configure Sensor Parameters**.
- 3 In **Sensor Parameters**, scroll through the list and select a parameter to view.
- 4 Click **OK** to close.

About port mapping

Symantec Network Security provides a way to tune the sensors to look for particular types of anomalies and signatures on a port by reconfiguring the default port mapping, or adding new mappings. For example, mappings can be added to run services on non-standard ports or to ignore ports on which you normally run non-standard protocols, to mitigate common violations of protocol from being falsely reported as events.

Viewing port mappings

The types of anomalies and signatures that the Symantec Network Security sensors look for on a port can be viewed in the Network Security console. With any user account, you can view the port mappings for any supported protocol.

To view port mappings

- 1 In the Network Security console, click **Configuration > Node > Port Mappings**.
- 2 In **Local Node Selection**, select the node for which you want to view the mappings.

About signature detection

Symantec Network Security provides the functionality to begin detection immediately by applying protection policies. In addition to this initial ability, detection can also be enhanced and tuned to a particular network environment by creating and applying user-defined signatures.

About Symantec signatures

Symantec Network Security uses network pattern matching, or signatures, to provide a powerful layer of detection. Signature detection involves detecting threats by looking for a specific pattern or fingerprint of a known bad or harmful thing. This known-bad pattern is called a signature. These patterns are traditionally based on the observed network behavior of a specific tool or tools.

Signature detection operates on the basic premise that each threat has some observable property that can be used to uniquely identify it. This can be based on any property of the particular network packet or packets that carry the threat. In some cases, this may be a literal string of characters found in one packet, or it may be a known sequence of packets that are seen together. In any case, every packet is compared against the pattern. Matches trigger an alert, while failure to match is processed as non-threatening traffic.

Symantec Network Security uses signatures as a compliment to PAD. The combination provides robust detection without the weaknesses of either PAD alone or signatures alone. Symantec Network Security's high performance is maintained by matching against the smallest set of signatures as is possible given the current context. Since many threats are detected and refined through the PAD functionality, Symantec Network Security minimizes the set of required signatures to maximize performance.

Symantec Network Security also uses methods of rapid response in creating signatures that detect attempts to exploit new vulnerabilities as soon as they hit the network, independent of the exploit tool. This results in earlier prevention of threats and more complete coverage.

About user-defined signatures

The Network Security console provides a way to configure and enable additional user-defined signatures on a per-sensor basis, as well as global signature variables, such as creating the variable name port to stand for a value of 2600. User-defined signatures are synchronized across clusters so that each node has the title, severity, and definition of the user-defined signature. SuperUsers can create, define, edit, and delete user-defined signatures. All users can view them.

Note: Both StandardUsers and RestrictedUsers can view user-defined signatures, but cannot add, edit, or delete them.

Viewing signatures

All users can view all available PAD event types and user-defined signatures from the Policies tab. You can also see which signatures are applied to the monitoring interfaces, interface pairs, or interface groups, as well as the list of signature variables.

To see interfaces

- ◆ On the **Policies** tab, click **Policies > Policies Applied to Interfaces** to see interfaces with policies applied.

To see applied signatures

- ◆ On the **Policies** tab, click **Policies > Policies** to see the Symantec signatures that are applied.

To see available signatures

- ◆ On the **Policies** tab, click the **User-defined Signatures** tab to see available user-defined signatures.

To see signature variables

- ◆ On the **Policies** tab, click the **Signature Variables** tab to see available variables to use when defining signatures.

About signature variables

Symantec Network Security provides signature variables for speed and accuracy, such as the variable name port to stand for a value of 2600. The signature variables apply globally to all signatures, both default Symantec signatures and any user-defined signatures.

To view signature variables

- ◆ On the **Policies** tab, click **Signature Variables > New**.

About refinement rules

Symantec Network Security detects both known and unknown (zero-day) attacks, using multiple detection technologies concurrently. Event refinement rules extend the Protocol Anomaly Detection capabilities. Symantec Network Security matches generic anomalies against a database of refinement rules, and for known attacks, reclassifies an anomaly event by retagging it with its specific name.

New refinement rules are available as part of SecurityUpdates on a periodic basis. Each software or appliance node downloads the refinement rules from LiveUpdate and stores them individually.

Incidents and Events

This chapter includes the following topics:

- [About incidents and events](#)
- [Monitoring incidents](#)
- [Monitoring events](#)
- [Managing the incident/event data](#)

About incidents and events

The Network Security console provides a central point from which you can monitor all attack activity in any network location defined in the topology tree. The Network Security console displays detailed information about incidents and events, which are the elements of a possible attack.

In the Network Security console, the Incidents tab displays both active and idle incidents and events taking place in the monitored network, and can be drilled down for multiple detail levels. Incidents to which no new events have been added for a given amount of time are considered idle, so Symantec Network Security closes them. The condition of the incident can be viewed in the State column of the Incidents table. The incident idle time is a configurable parameter.

An incident is a set of events that are related. An event is a significant security occurrence that appears to exploit a vulnerability of the system or application. When a sensor detects a suspicious event, it sends the data to be analyzed. The analysis process correlates the event with similar or related events, and categorizes them in the form of an incident. The incident is named after the event with the highest priority, and reported in the form of incidents that are displayed in the Network Security console.

About the Devices tab

The Devices tab provides a tree-oriented view of the network topology with a detailed summary of each device. When you select an object from the topology tree in the left pane, the right pane displays related information. Symantec Network Security updates this information at frequent intervals, so the status remains current.

Viewing device details

When you select an object in the Devices tab, the right pane displays information about that object. Depending on the selected object, the following information can appear in the right pane:

- **Device Type:** Displays the type of device selected.
- **IP address:** Displays the IP address of the selected device, or the management IP address for a device with multiple IP addresses.
- **Node Number:** Displays the node number assigned to the software or appliance node, between 1 and 120.
- **Customer ID:** Displays an optional user-defined ID. Customer IDs for in-line pairs and interface groups reflect the 7100 Series appliance nodes to which they belong.
- **Model:** Displays the model number of a 7100 Series appliance, either 7120, 7160, or 7161.
- **Monitoring Group:** Identifies the monitoring group of the selected device, if any.
- **Monitored Networks:** Identifies the networks for which port usage patterns are tracked and anomalies detected. Displayed only if you entered network IP addresses on the Network tab when editing interfaces, adding in-line pairs, or adding interface groups. Available only on 7100 Series interfaces.
- **TCP Reset Interface:** Displays the interface that sends TCP resets; either eth0, eth1, or eth2, corresponding to your choice of RST0, RST1, or RST2 when you added the interface group.
- **Bandwidth:** Displays the expected throughput for the selected object.
- **Sensor Status:** Displays the current status of the related sensor.
- **Description:** Displays a brief optional description of the object.
- **Active Security Incidents:** Displays the active incidents of the selected topology object, with name, state, node number, and last date modified.

Viewing interface details

If you click on a monitoring interface object in the Devices tab, the Details of Selected Topology Object dialog box displays the following information:

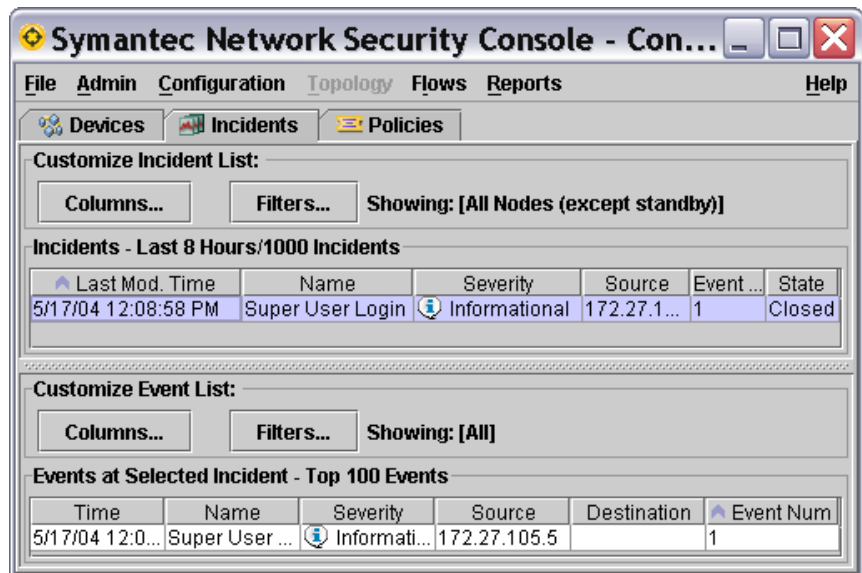
- **Customer ID:** Displays the customer ID that you assigned to the monitored interface.
- **Interface Name:** Displays the name of the interface on the software or appliance node to which the monitored interface sends copied data.
- **Media Type:** Displays the type of link being monitored, either Ethernet or gigabit.
- **Flow Collection:** Displays whether flow status collection is enabled on the monitored interface.
- **Capture Packet Mode:** Displays whether packet capture mode is enabled on the monitored interface. A value of Header Only indicates that packet capture is not enabled. A value of Entire Packet indicates packet capture is enabled.
- **Description:** Displays the optional description of what is happening.
- **Sensor running message:** Displays whether the sensor is running on the Network Security interface to the monitored interface.
- **Bit rate:** Displays the average number of megabits per second (Mbps) monitored on the interface. This calculation is based on payload, which may differ slightly from the bit rate calculation on a particular switch or router.
- **Packet rate:** Displays the number of packets per second (pps) monitored on the interface.
- **Percent of packets dropped:** Displays the average percent of packets that are not being monitored on the interface.
- **Aggregate bit rate:** Displays the aggregate number of megabits per second (Mbps) monitored on the gigabit interface.
- **Aggregate packet rate:** Displays the aggregate number of packets per second (pps) monitored on the gigabit interface.
- **Percent of total traffic per sensor:** Displays the percentage of traffic being sent to each sensor sub-instance monitoring a gigabit link. For example, if you have 500 Mbps of aggregate bit rate traffic, and Sensor 1 is monitoring 15% of the total traffic, then Sensor 1 is monitoring $500 \text{ Mbps} \times .15 = 75 \text{ Mbps}$.
- **Logged Event Count:** Displays the number of events associated with this incident that have been logged to the database.

About the Incidents tab

The Network Security console displays incident and event data in the following:

- **Incidents tab:** Displays both active and idle incidents. When you select an incident, Events At Selected Incident in the lower pane displays information about the related events.
- **Devices tab:** Displays the topology tree. When you select an object in the topology tree, the Network Security console displays related information in the right pane, including a link to security incidents that are currently active on that object.

The Incidents tab provides a multi-level view of both incidents and events. Incidents are groups of multiple related base events. Base events are the representation of individual occurrences, either suspicious or operational. The sensors notify the software or appliance node of any suspicious actions or occurrences that might warrant a response, such as a probe. Symantec Network Security also monitors operational occurrences that the user should be aware of, such as a Symantec Network Security license approaching the expiration date.



The Incidents tab contains an upper and lower pane: **Incidents**, and **Events at Selected Incident**. The upper pane displays information about each incident, taken from the highest-priority event within that incident. The values may change if an event of higher priority is added to the same incident.

To view incident data

- ◆ In the Network Security console, click the **Incidents** tab.

All users can modify the view by adjusting font size, selecting and sorting columns, and/or applying filters.

Viewing priority color codes

All users can sort the incident data by clicking on the column heading. The toggle sorts the column in ascending or descending order.

To sort the incidents

- ◆ Do one of the following:
 - Click the heading of the column you want to sort.
 - Click the column heading again to reverse the order.

Annotating incidents and events

You can add comments to incidents and events. Each annotation receives a time stamp and lists the author of the annotation. You can sort multiple annotations for an event by time stamp in ascending or descending order.

To annotate an incident or event

- 1 On the **Incidents** tab, double-click an incident or event.
- 2 Click **Analyst Note**.
- 3 Enter the information relevant to this incident.
The **Note** field can include guidelines established by the SuperUser, such as ticket number, owner, and the last action taken in response to the event.
- 4 Click **Add Note** to preserve your annotation.
- 5 In **Analyst Note**, click **Close** to save and close.

Marking incidents as viewed

All users can mark incidents to distinguish new incidents from reviewed incidents.

To mark incidents already viewed

- 1 On the **Incidents** tab, right-click an incident.
- 2 In the pop-up list, click **Mark Incident**.
The Marked column of the incident displays a red hash mark to indicate that it has been viewed.



Note: If an incident changes after it was marked, such as a new event being added to it, the red hash mark changes to a red circle to flag you.

Monitoring incidents

An incident is a set of events that are related. An event is a significant security occurrence that appears to exploit a vulnerability of the system or application. When a sensor detects a suspicious event, it sends the data to be analyzed. The analysis process correlates the event with similar or related events, and categorizes them in the form of an incident. The incident is named after the event with the highest priority, and reported in the form of incidents that are displayed in the Network Security console.

Viewing incident data

The Incidents tab contains an upper and lower pane: **Incidents**, and **Events at Selected Incident**. In the upper pane, information about each incident is displayed. This information is taken from the highest-priority event within that incident. Therefore, the values may change if an event of higher priority is added to the same incident.

To view incident data

- ◆ In the Network Security console, click the **Incidents** tab.

Selecting incident columns

Not all incidents contain data in every category, so you may want to remove empty columns or add others to customize the display. All users can modify the display of incident data by selecting columns.

To customize the incident columns

- 1 On the **Incidents** tab, in the upper **Incidents** pane, click **Columns**.
- 2 In **Table Column Chooser**, do one of the following:
 - Click **Select All** to display all columns.
 - Click the individual columns that you want to view.
- 3 Click **OK** to save and close.

The Incidents tab can display the following incident data:

- **Last Mod. Time** Indicates the date and time when Symantec Network Security last modified the incident record.
- **Name** Indicates the user group of the current user.
- **Severity** Indicates the severity level assigned to the incident. An incident's severity is a measure of the potential damage that it can cause.
- **Source** Indicates the IP address of the attack source. If the source is made up of multiple addresses, then the Network Security console displays (multiple IPs) and you can view the list of addresses by double-clicking the event to see Event Details.
- **Destination** Indicates the IP address of the attack target. If the destination is made up of multiple addresses, then the Network Security console displays (multiple IPs) and you can view the list of addresses by double-clicking the event to see Event Details.
- **Event Count** Indicates the total number of events associated with this incident that have been logged to the database.
- **Device Name** Indicates the name of the device where the incident was detected.
- **Location** Indicates the location of the device where the incident was detected.
- **State** Indicates the condition of the incident, either Active or Closed. Incidents to which no new events have been added for a given amount of time are considered idle, and Symantec Network Security closes them.
- **Marked** Indicates whether you marked the incident as viewed.
- **Node #** Indicates the number of the software or appliance node that detected the incident.
- **Node Name** Indicates the name of the software or appliance node that detected the incident.
- **Other Node #s** Indicates the numbers of the software or appliance node that the incident was cross-node correlated to, if any.

See the following related information:

- See [“About incidents and events”](#) on page 91.
- See [“Selecting event columns”](#) on page 100.

- See [“Marking incidents as viewed”](#) on page 95.

Filtering the view of incidents

You can filter the view of incident data to provide a shorter list to sift through, using the Incident Filter. For example, you can set the Incidents table to display only active incidents. You can choose between viewing the incidents detected by all software and appliance nodes, and viewing only those detected by a particular software or appliance node. By default, incidents from all nodes are displayed.

Note: When you apply incident view filters, they apply only to the incidents, not to the events correlated to the incidents. For example, even if you select the **Sensor Only** filter, an operational event that is correlated to a sensor incident will still be displayed.

To filter the view of incidents or events

- 1 In the **Incidents** tab, in the upper **Incidents** pane, click **Filters**.
- 2 Click **Hide Closed Incidents** to show only active incidents in the cluster.
- 3 In **Incident Class**, do one of the following:
 - Click **Hide All Operational** to show only those incidents classified as sensor events, and filter out all operational notice events.
 - Click **Hide Sensor** to show only operational events, such as Network Security console logins.
 - Click **Show All Operational and Sensor** to show both operational and sensor events.
- 4 In **Marked State**, do one of the following:
 - Click **Hide Unmarked** to show only the incidents that have been marked in the Network Security console.
 - Click **Hide Marked** to show only the incidents that have not been marked in the Network Security console.
 - Click **Show Both** to include both marked and unmarked incidents.
- 5 In **Analyst Notes**, do one of the following:
 - Click **Hide Unannotated** to show only incidents with annotations and incidents that contain events with annotations.
 - Click **Hide Annotated** to show only incidents that do not have annotations or that contain events with annotations.
 - Click **Show Both** to include both annotated and unannotated incidents.

- 6 In **Node List**, do one of the following:
 - In **Show Incidents from Node #**, click **1** from the pull-down list to show only incidents from the selected software or appliance node, or **All (except standby)** to view incidents from all the software or appliance nodes within the topology excluding standby nodes.
 - Click **Include Backup Nodes** to preserve incidents during a failover scenario.
- 7 In **Incident Hours**, do one of the following:
 - In **Maximum Incident Hours to Display**, enter a value to limit the total number of hours.
 - In **Maximum Incidents Within Incident Hours**, enter a value to limit the total number of incidents within the hour limit.
- 8 Click **Apply** to save and exit.

See the following for related information:

- See [“Marking incidents as viewed”](#) on page 95.

Monitoring events

An incident is a possible attack composed of multiple related events. When the sensor detects a suspicious event, it correlates the event to an incident containing related events. Event types are group names for one or more base events. Incidents consist of one or more event types, and event types consist of one or more base events. The Network Security console displays event data in the lower pane below the Incident table.

With any account, you can annotate events and mark incidents to improve incident tracking, management, assignment, and response to enterprise threats.

Viewing event data

The Incidents tab contains an upper and lower pane: **Incidents**, and **Events at Selected Incident**. In the upper pane, information about each incident is displayed. View the event data that is specific to a particular incident by clicking the respective incident row. The related event information is then displayed in the lower pane.

To view event data

- 1 In the **Incidents** tab, click an incident row.
- 2 Related events are displayed in the lower **Events at Selected Incident** pane.

Note: Both StandardUsers and RestrictedUsers can modify the view by selecting which columns to display, sorting columns, and applying view filters.

Selecting event columns

Not all events contain data in every category, so you may want to remove empty or irrelevant columns, or add others to customize the display. All users can modify the display of event information by selecting columns.

To select event columns

- 1 In the **Incidents** tab, in the lower **Events at Selected Incidents** pane, click **Columns**.
- 2 In **Table Column Chooser**, do one of the following:
 - Click **Select All** to select all columns.
 - Click the individual columns you want to view.
- 3 Click **OK** to save and close.

The **Events at Selected Incident** can display the following information:

- **Time** Indicates the date and time when Symantec Network Security first detected and logged the event.
- **Event Type** Indicates the event category of the detected event.
- **Name** Indicates the user group of the current user.
- **Source** Indicates the IP address of the packet that triggered the event. If the source is made up of multiple addresses, then the Network Security console displays (multiple IPs) and you can view the list of addresses by double-clicking the event to see Event Details.
- **Destination** Indicates the IP address of the attack target. If the destination is made up of multiple addresses, then the Network Security console displays (multiple IPs) and you can view the list of addresses by double-clicking the event to see Event Details.
- **Severity** Indicates the severity level assigned to the event. An event's severity is a measure of the potential damage that it can cause.

- **Confidence** Indicates the confidence level assigned to the event. An event's confidence is a measure of the level of certainty that it is actually part of an attack. If the event is merely suspicious, then it is assigned a lower confidence level. If Symantec Network Security collects more data on the event to substantiate its confidence, the confidence is adjusted upward.
- **Event Number** Indicates the order in which the event was added to the incident.
- **Device Name** Indicates the name of the device where the event was detected.
- **Interface Group** Indicates the name of the interface group where the event was detected.
- **Location** Indicates the location of the device where the event was detected.
- **VLAN ID** Indicates the identification of the VLAN where the event was detected.
- **Blocked** Indicates whether the event was blocked or not. You can block events only with a 7100 Series appliance node.

Note: Both StandardUsers and RestrictedUsers can modify the display of event information by selecting which columns to display, sorting columns, and applying view filters.

Filtering the view of events

You can filter the event data that is displayed by using the Event Filter.

To filter the view of events

- 1 On the **Incidents** tab, in the **Events at Selected Incident** pane, click **Filters**.
- 2 In **Event Class**, do one of the following:
 - Click **Hide Operational** to show only those events classified as sensor events.
 - Click **Hide Sensor** to show only events associated with notices.
 - Click **Show Both** to show all events relating to the selected incident.
- 3 In **Maximum Events to Display**, enter a value. The default is 100 events per incident.
- 4 Click **Apply** to save and exit.

Viewing event notices

Symantec Network Security monitors operational events as they are processing, such as startup and shutdown of a software or appliance node, or errors experienced within a module. The Incidents tab displays notices about the following types of operational events:

- **Monitored Host Unavailable:** Symantec Network Security has detected a drop in network availability.
- **iButton Token Failure:** The iButton, used only by Network Security software nodes, stores the private key portion of the Symantec Network Security signature certificate to safeguard the private key against being stolen or compromised. The iButton also confirms the identity of a software node.

Note: Notify us of your iButton’s impending expiration. Replace it before it expires to ensure that the log files continue to be signed and the iButton can continue to perform its authentication and data hashing functions. See the *Symantec Network Security Installation Guide* for instructions on iButton replacement.

- **iButton Certificate Expiration:** Several times during the 30 days prior to the expiration of your encryption certificate, warnings of the impending expiration are displayed in the Active Incidents tab. The notices are sent every 6 hours. The priority of the notices increases as the certificate lifetime gets shorter:

Lifetime	Priority
life < 1 hour	Critical
1 hour =< life < 1 day	Urgent
1 day =< life < 3 days	High
3 days =< life < 1 week	Medium
1 week =< life < 1 month	Low

Warnings of the impending expiration are displayed in the Active Incidents tab. Expiration dates are also displayed when Symantec Network Security is restarted.

- **Network Security SuperUser Login:** Symantec Network Security displays this event whenever a SuperUser logs into the Network Security console.

- **Network Security Administrator Login:** Symantec Network Security displays this event whenever an Administrator logs into the Network Security console.
- **Network Security StandardUser Login:** Symantec Network Security displays this event whenever a StandardUser logs into the Network Security console.
- **Network Security RestrictedUser Login:** Symantec Network Security displays this event whenever a RestrictedUser logs into the Network Security console.
- **Email Initiation Request Failed:** An error occurred while sending an email notification from Symantec Network Security.
- **Successful Email:** An email response was successfully sent by Symantec Network Security.
- **SNMP Initiation Request Failed:** An error occurred while sending an SNMP trap from Symantec Network Security.
- **Email Alert Failed:** An error occurred while sending an email alert from Symantec Network Security.
- **SNMP Alert Successful, but Truncated:** An SNMP trap was successfully sent by Symantec Network Security, but the message was too long and was truncated.
- **SNMP Alert Failed:** An error occurred while sending an SNMP alert from Symantec Network Security.
- **Unable to Execute Custom Response Process:** Failed to execute custom response to an event.
- **Disk Space Warning:** Symantec Network Security displays this event whenever <100,000 blocks and <10% of disk space is available.
- **Failover Active:** Symantec Network Security displays this event whenever a software or appliance node with failover enabled becomes the active node.

Managing the incident/event data

All users can manage the information that is displayed on the Network Security console by selecting columns, sorting, filtering, and limiting the size of tables. You can also annotate, mark, save, print, and email incident and event data.

Loading cross-node correlated events

If the selected incident is correlated to an incident from another software or appliance node (as denoted in the **Other Node #** column), then each tab of Incident details will contain one sub-incident of the cross-node incident, and the tab will carry the name of the node that detected that sub-incident.

To load events

- ◆ Click **Load Events** to load the events for the currently selected sub-incident. Load Events will be disabled if the currently selected sub-incident's events are already loaded.

Saving, printing, or emailing incidents

All users can view details, save, print, or email incident data, or send it to the clipboard for pasting, together with its associated events, from the Network Security console. You can display the options by double-clicking an incident row and choosing from the menu items on the Incident Details, or by right-clicking an incident row, and choosing from the menu items displayed.

Viewing incident details

Symantec Network Security provides a deeper level of information about each incident from the Incidents tab.

To view incident details

- 1 In the Network Security console, click the **Incident** tab.
- 2 In **Incidents**, double-click any incident row.
- 3 In **Incident Details**, click **Top Event** to view the highest priority event correlated to that incident.

Incident Details can display the following information:

■ Event Mapped Type	The event type to which the base event is mapped.
■ Base Event Type	The base event mapped to the incident's highest priority event.
■ Incident ID	Unique incident identifier assigned to the incident by Network Security.
■ Network Security software node	The name of the Network Security software node on which the incident was detected.

■ Customer ID	This is the customer ID entered in the topology for the interface where the event was detected.
■ End Time	The time at which Network Security stopped monitoring the event.
■ CVE Number	The CVE (Common Vulnerabilities and Exposures) number, if any. CVE numbers are a list of standardized names for vulnerabilities and other information security exposures compiled by the MITRE Corporation. For a complete list of CVE numbers, see http://cve.mitre.org .
■ Priority	The priority level assigned to the incident by the Analysis Framework. The priority level is a function of the severity and reliability levels.
■ Severity	The severity level Network Security assigned to the incident. An incident's severity is a measure of the potential damage that an incident can cause. Severity levels range from 0 to 255, with 255 as the most severe.
■ Reliability	The reliability level Network Security assigned to the incident. The reliability value indicates the level of certainty that a particular incident is actually an attack. If the incident is merely suspicious, then its assigned reliability level is low. If Network Security collects more data on the incident to substantiate its reliability, the reliability is adjusted upward. Reliability levels range from 0 to 255, with 255 as the most reliable.
■ Attack Source(s)	The IP address of the packet that triggered the event. Click the address to view related host name or flow statistics.
■ Attack Destination(s)	The IP address of the event's target. Click the address to view related host name or flow statistics.

Note: StandardUsers can view detailed information about each incident; RestrictedUsers cannot.

Saving incident data

All users can save detailed information about each incident on the Network Security console Incidents tab.

To save incident data

- 1 In the Network Security console, click the **Incidents** tab.

- 2 Right-click an incident row, and click **Save**.
- 3 Choose a file format from the following:
 - Click **Save as PDF**.
 - Click **Save as HTML**.
 - Click **Save as PS**.
- 4 Enter the desired filename, and click **Save**.

Printing incident data

All users can print detailed information about each incident on the Network Security console Incidents tab.

To print incident data

- 1 In the Network Security console, click the **Incidents** tab.
- 2 Right-click an incident row, and click **Print**.
- 3 Optionally, you can choose from the following print options:
 - Click **Page Setup** to layout the page before printing or previewing.
 - Click **Print Preview** to preview the page before printing.
- 4 Click **Print** to send the incident data to a printer.

Configuring Network Security to email

All users can configure a Network Security console to email detailed information about each incident on the Incidents tab.

To configure Network Security to email incident data

- 1 In the Network Security console, click the **Incidents** tab.
- 2 Right-click an incident row, and click **Email > Configuration**.
- 3 In **Email Configuration**, indicate the following:
 - In **Mail Server**, enter your SMTP server for outgoing emails.
 - In **To**, enter the destination.
 - In **From**, enter the email source.
 - In **Subject**, enter the email subject.

This information is stored in User Preferences.

Emailing incident data

All users can send detailed information about each incident via email, on the Network Security console Incidents tab.

To email incident data

- 1 In the Network Security console, click the **Incidents** tab.
- 2 Right-click an incident row, and click **Email**.
- 3 If you want to send without editing, do one of the following:
 - Click **Send Directly > in HTML** to send an email in HTML format.
 - Click **Send Directly > in Text** to send an email in plain text format.
- 4 If you want to edit before sending, do one of the following:
 - Click **Compose > in HTML** to send an email in HTML format.
 - Click **Compose > in Text** to send an email in plain text format.

After the incident content loads into the email, edit or add to the content, and click **Send**.
- 5 Select a path by doing one of the following:
 - Click **Email > Through Browser** to select a browser path and store it in Local Preferences for future reference.
 - Click **Email > Through Mail Client** to select a mail client path and store it in Local Preferences for future reference.
- 6 Click **Email > SMTP Mail Server** to select a mail server and store it in Local Preferences for future reference.

Note: This SMTP mail server is used by the Network Security console, which may or may not be the SMTP mail server used by the Network Security software node. Setting the SMTP Server notification parameter does not necessarily affect the SMTP mail server referenced in this procedure.

Pasting incident data

All users can copy and paste detailed information about each incident into another format, on the Network Security console Incidents tab.

To copy and paste incident data

- 1 In the Network Security console, click the **Incidents** tab.
- 2 Right-click an incident row, and click **To Clipboard**.

- 3 Open the desired email or file, and paste the incident data from the clipboard to the email content.

Reports and Queries

This chapter includes the following topics:

- [About reports](#)
- [Reporting via the Network Security console](#)
- [About top-level report types](#)
- [About querying flows](#)

About reports

Symantec Network Security provides a comprehensive reporting module that can automatically generate and send daily email reports of the most frequently occurring event types for the day. Pre-defined report types with drill-down data retrieval and dynamic chart and graph generation aid reporting and provide a clear picture of network events. These reports provide detailed data on the types of events and incidents that occurred, and protocols exploited during the specified time period. With any account, you can view and print reports, and save them in multiple formats. You can generate reports that appear in table format, and sort the table columns.

Symantec Network Security can generate email reports of incidents logged for all Network Security software nodes in the cluster. You can also generate reports on demand about any Network Security software nodes in the cluster. These Network Security console reports are available as top-level reports and as drill-down reports.

Reporting via the Network Security console

On the Reporting menu, the Network Security console lists top-level reports. In most top-level reports, you can generate one or more levels of drill-down reports that provide a more focused level of detail. By supplying report parameters, you

can choose the report type. The types of reports that Symantec Network Security generates are described in detail in the following sections.

In addition to scheduled reports, you can generate various report types on demand. Symantec Network Security generates reports from data collected from all Network Security software nodes in the cluster. You can supply various report parameters, depending on the type of report, such as start and end dates and times.

About report formats

The reports are generated in one or more formats, depending on the type of report. Possible formats include tables, bar charts, column charts, and pie charts. The report generator makes most reports available in more than one format. All users can navigate from one format to another by selecting one of the report formats listed in the drop-down menu in the upper right corner of the report window.

About top-level report types

This section describes the following top-level reports that Symantec Network Security generates, most of which also include drill-down reports:

- [Reports of top events](#)
- [Reports per incident schedule](#)
- [Reports per event schedule](#)
- [Reports by event characteristics](#)
- [Reports per Network Security device](#)
- [Drill-down-only reports](#)

Reports of top events

Symantec Network Security generates the following top-level event reports:

Table 9-1 Types of top-level event reports

Type	Description
Top event types	The Top Event Types report lists the event types, such as Synflood, Telnet DoS and Portscan, that occurred most frequently during the specified time period, and the number of times each event type occurred. Also specify the maximum number of unique event types to display. For example, generate a report on the top 10 unique events or top 100 unique events. To view the number of times any event type occurred, hover the cursor over the event. Symantec Network Security generates the Top Event Types report in the table, pie chart and bar chart formats. You can generate several drill-down reports for each event type listed in the Top Event Type report.
Top event destinations	The Top Event Destinations report lists the most frequently occurring destination IP addresses of detected events. However, the top event destinations do not necessarily map to the top event types. You must specify the report start and end date/time, and number of unique addresses to display. For example, you could generate a report on the top 10 addresses or top 100 addresses. Symantec Network Security generates the Top Event Type report in the table, pie chart and bar chart formats. To view the number of times an IP address was an event destination during the report time period, hover the cursor over the table row, pie piece, or bar corresponding to the event destination. You can generate several drill-down reports for each event type listed in the Top Event Destinations report.
Top event sources	The Top Event Sources report lists the IP addresses that were most frequently the source addresses of detected events. You specify the report start and end date/time, and the maximum number of unique addresses to display. Symantec Network Security generates this report in the table, pie chart and bar chart formats. To view the number of times an event source occurred during the report time period, hover the cursor over the table row, pie piece or bar corresponding to the event source. You can generate several drill-down reports for each event type listed in the Top Event Sources report.

Reports per incident schedule

Symantec Network Security generates the following types of incident reports:

Table 9-2 Types of incident reports

Type	Description
Incidents per month	This reports displays the total number of incidents that occurred during each month of the time period you specify. If a month is not listed in the report, then no incidents were detected during that month. Symantec Network Security generates this report in table and column chart formats. You can generate several drill-down reports for each month listed in the Incidents Per Month report.
Incidents per day	This reports displays the total number of incidents that occurred per day during the time period you specify. If a day is not listed in the report, then no incidents were detected during that day. Symantec Network Security generates this report in table and column chart formats. You can generate several drill-down reports for each day listed in the Incidents Per Day report.
Incidents per hour	This report displays the total number of incidents that occurred per hour during the time period you specify. If an hour is not listed in the report, then no incidents were detected during that hour. The Incidents Per Hour report is generated in table and column chart formats. You can generate several drill-down reports for each hour listed in the Incidents Per Hour report.
Incident list	For each incident that occurred during the report period you specify, this report lists the incident start date and time, event type to which the incident is mapped, the name of the device where Symantec Network Security detected the incident, and the number of the Network Security software node that detected the incident. Symantec Network Security generates this report in table format only. You can generate several drill-down reports for each incident listed in the Incident List report.

Reports per event schedule

Symantec Network Security generates the following types of event reports:

Table 9-3 Types of event reports

Type	Description
Events per month	This report displays the total number of events detected per month during the time period you specify. If a month is not listed in the report, then no events were detected during that month. Symantec Network Security generates this report in table and column chart formats. You can generate several drill-down reports for each month listed in the Events Per Month report.
Events per day	This report displays the total number of events detected per day during the time period you specify. If a day is not listed in the report, then no events were detected during that day. Symantec Network Security generates this report in table and column chart formats. You can generate several drill-down reports for each day listed in the Events Per Day report.
Events per hour	This report displays the total number of events detected per hour during the time period you specify. If an hour is not listed in the report, then no events were detected during that hour. Symantec Network Security generates this report in table and column chart formats. You can generate several drill-down reports for each hour listed in the Events Per Hour report.

Reports by event characteristics

Symantec Network Security generates the following types of event reports:

Table 9-4 Types of event reports

Type	Description
Events by classful destination	This report sorts events by their destination IP addresses, and presents a count of the number of addresses that are from class A, class B and class C networks. Specify report start and end dates/times, and maximum number to display. This report is generated in table, column and bar chart formats. This report has no drill-down reports.

Table 9-4 Types of event reports

Type	Description
Events by classful source	This report sorts events by their source IP addresses and presents a count of the number of addresses that are from class A, class B and class C networks. Specify report start and end dates/times, and maximum number to display. This report is generated in table, column and bar chart formats. This report has no drill-down reports.
Events by protocol	This report lists the number of events detected that exploit each particular protocol, such as ICMP, UDP, TCP, or IP. You specify the report start and end dates/times. Symantec Network Security generates this report in table, bar, column and pie chart formats. This report has no drill-down reports.
Events by vendor	This report lists the number of events detected per vendor. For example, signatures detected by Symantec Network Security are grouped as RCRS events because RCRS is the vendor ID for Symantec Network Security. You specify the report start and end dates/times. Symantec Network Security generates this report in table, bar, column and pie chart formats. This report has no drill-down reports.
Destinations of source	This report lists the destination IP address(es) for any event source IP address you specify, and the number of times each address was the destination for the source address. You also specify the report start and end dates/times. This report is generated in table and bar chart formats. You can generate several drill-down reports from the Destinations of Source report.
Sources of destination	This report lists the source IP address(es) for any event destination IP address you specify, and the number of times each address was the source for the destination address. Specify the report start and end dates/times, and destination address. This report is generated in table and bar chart formats. You can generate several drill-down reports from the Sources of Destination report.
Events by VLAN ID	This report lists all events for all VLAN IDs. If the VLAN ID has not been set up, the report lists any unknown VLAN IDs as -1. You can generate drill-down event types for each VLAN ID, and further, to the event list.
Events by device	This report lists all events for all devices and interfaces in the network topology. You can generate drill-down event types by interface.

Table 9-4 Types of event reports

Type	Description
Event list by destination IP	This report lists all events by destination IP address for all devices and interfaces in the network topology. You can generate drill-down event lists by destination IP from Top Event Destinations.
Event list by source IP	This report lists all events by source IP address for all devices and interfaces in the network topology. You can generate drill-down event lists by source IP from Top Event Sources.

Reports per Network Security device

Symantec Network Security generates the following types of device reports:

Table 9-5 Types of device reports

Type	Description
Network Security login history	This report lists the user login times, IP addresses from which the user logged in, and the type of user that logged in, either a SuperUser with full read/write privileges, or one of the other user login accounts with limited permissions. Specify the report start and end dates/times. This report is generated in table format only. This report has no drill-down reports.
Network Security operational events	This report lists operational events such as user logins, communication errors, response actions, and license status notifications. This report allows you to drill-down to event details.
Devices with flow statistics	This report lists names for devices on which the Flow Status Collection sensor mode is enabled, and the number of the software or appliance node where the sensor is located. Symantec Network Security generates this report in table format only. With a SuperUser, Administrator, or StandardUser account, you can generate several drill-down reports for details on sources and destination IP addresses and ports for the flows, as well as flow protocols.

Note: StandardUser can generate reports from devices with flow statistics; RestrictedUser are not.

Drill-down-only reports

Most top-level report types are also available as drill-down reports within other top-level reports. However, some Network Security console reports are accessible only as drill-down reports from within top-level reports or other drill-down reports. This section describes the following drill-down-only reports.

For the incident you select, data is displayed within the Incident List report.

Table 9-6 Drill-down-only reports

Report	Description
Incident details	This report lists all the events contained in the selected incident or time period, as well as the event end time, the event source and destination IP addresses, and the name of the device where the event was detected. Symantec Network Security generates the Event List report in table format only. You can access this report from within any Incidents or Events report, as well as from within the Top Event Destination and Top Event Source reports.
Event list	For the incident you select, data is displayed within the Incident List report.
Events details	The Event Details report displays the data within any Event List report.
Sources of event	The Sources of Event report lists all of the source IP addresses for the event you select. Symantec Network Security generates this report in table, pie chart and bar chart formats. You can generate this report from within the Top Event Types report.
Destinations of event	The Destinations of Event report lists all of the destination IP addresses for the event you select. Symantec Network Security generates this report in table, pie chart and bar chart formats. You can generate this report from within the Top Event Types report.
Flows by source address	This report lists the source IP addresses of flows found on devices with the Flow Status Collection sensor mode enabled. You can generate this report from within the Devices with Flow Statistics report.
Flows by destination address	This report lists the destination IP addresses of flows found on devices with Flow Status Collection sensor mode enabled. You can generate this report from within the Devices with Flow Statistics report.

Table 9-6 Drill-down-only reports

Report	Description
Flows by source port	This report lists the source ports of flows found on devices with Flow Status Collection sensor mode enabled. You can generate this report from within the Devices with Flow Statistics report.
Flows by destination port	This report lists the destination ports of flows found on devices with Flow Status Collection sensor mode enabled. You can generate this report from within the Devices with Flow Statistics report.
Flows by protocol	This report lists the protocols of flows found on devices with Flow Status Collection sensor mode enabled. You can generate this report from within the Devices with Flow Statistics report.

About querying flows

FlowChaser serves as a data source in coordination with Symantec Network Security TrackBack, a response mechanism that traces a DoS attack or network flow back to its source. The FlowChaser database can be queried for flows by port and arbitrary address. The Network Security console displays both current flow data and exported flow data, and provides secondary query options from the results page.

Symantec Network Security provides query options as follows:

- In Query Current Flows or Query Exported Flows
- In Event Details, right-click the IP address to see the flow statistics
- In Event Details of an Exported Related Flows, exported flows are displayed

The Network Security console retrieves a limited number of records for each query, which prevents overloading memory, and displays the results in a table. If more results are available, click Next Results to proceed.

Viewing current flows

View Current Flows enables you to search against all of the collected flows by FlowChaser. These flows are stored in memory so they are not persistent.

To query current flows

- 1 In the Network Security console, click **Flow** > **View Current Flows**.

- 2 Choose one of the following tabs:
 - **Match Source and Destination:** This will make a more focused query on specific source and destination IPs.
 - **Match Source or Destination:** This will make a broader query on either a source IP or a destination IP.
 - 3 In **Match Source and Destination**, send a focused query to display only flows that pertain to specific source IPs and destination IPs by entering data in the following fields:
 - **Source IP:** Numeric IP address
 - **Prefix Len:** Mask of the IP address in integers between 1 and 32
 - **Port:** Valid port number
 - **Destination IP:** Numeric IP address
 - **Prefix Len:** Mask of the IP address in integers between 1 and 32
 - 4 In **Match Source or Destination**, send a broader query to display flows that pertain to either a source IP or a destination IP by entering data in the following fields:
 - **Source or Destination IP:** Numeric IP address
 - **Prefix Len:** Mask of the IP address in integers between 1 and 32
 - **Port:** Valid port number
-
- Note:** The Network Security console displays the flow data in table format, one page at a time. To sort the table, click the heading of any column. This sort, however, applies only to the page currently displayed, which may be only a portion of the entire report. At the top of the display, a prompt indicates how many flows are currently displayed, out of the total report.
-
- 5 Do one of the following:
 - Click **Start Query** to run a flow query based on the parameters that you configured.
 - Click **Next Results** to view the next page of a query that was too large to display in its entirety.
 - Click **Clear** to stop the active query and remove the results from display.

Note: StandardUsers can query the FlowChaser database for current or exported flow data; RestrictedUsers cannot.

Viewing exported flows

Query Exported Flows enables you to search against flow data that has been logged to the disk database. This enables flow data to be saved when a certain condition is triggered. The result is that a new event appears in the Network Security console with a link to the actual flow data. The search dialog allows the user to search across all the flows that have been exported.

To query exported flows

- 1 In the Network Security console, click **Flows > View Exported Flows**.
- 2 Choose one of the following tabs:
 - **Match Source and Destination:** This will make a more focused query on specific source and destination IPs.
 - **Match Source or Destination:** This will make a broader query on either a source IP or a destination IP.
- 3 In **Match Source and Destination**, you can display only flows that pertain to specific source and destination IPs. To make this more focused query, enter data in the following fields:
 - **Source IP:** Numeric IP address
 - **Port:** Valid port number
- 4 In **Match Source or Destination**, you can display flows that pertain to either a source IP or a destination IP. To make this broader query, enter data in the following fields:
 - **Source or Destination IP:** Numeric IP address
 - **Port:** Valid port number

Note: The Network Security console displays the flow data in table format, one page at a time. You can sort the table by clicking the heading of any column. This sort, however, applies only to the page currently displayed, which may be only a portion of the entire report. At the top of the display, a prompt indicates how many flows are currently displayed, out of the total report.

- 5 Do one of the following:
 - Click **Start Query** to run a flow query based on the parameters that you configured.
 - Click **Next Results** to view the next page of a query that was too large to display in its entirety.
 - Click **Clear** to stop the active query and remove the results from display.

Note: StandardUsers can query the FlowChaser database for current or exported flow data; RestrictedUsers cannot.

Log Files

This chapter includes the following topics:

- [About the log files](#)
- [About log files](#)

About the log files

Symantec Network Security maintains multiple logging databases and tools to view, compress, and archive them.

The Symantec Network Security software and the Symantec Network Security 7100 Series appliance employ a common core architecture that provides detection, analysis, storage, and response functionality. Most procedures in this section apply to both the 7100 Series appliance and the Symantec Network Security 4.0 software. The 7100 Series appliance also provides additional functionality that is unique to an appliance. Each section describes this additional functionality in detail.

This section describes the following:

- [About the install log](#)
- [About the operational log](#)

About the install log

Symantec Network Security creates an install log that records all of the parameters entered during the installation procedure. The Network Security console provides a view of the install log file of each node via Admin > Node > Manage Logs, which displays the date and time of installation.

About the operational log

The operational log records events that Symantec Network Security is processing, such as startup and shutdown of the Network Security software or appliance node, or errors experienced within the node. The Network Security console provides a view of the operational log file of each node via Admin > Node > Manage Logs.

All actions or modifications made in the Network Security console to a software or appliance node are logged to the operational log file, which includes information such as the date and time, name, type of modification, and other data specific to the modification.

About log files

Symantec Network Security provides log and database management from the Network Security console, described in the following sections:

- [Viewing log files](#)
- [Viewing live log files](#)

Note: Both StandardUsers and RestrictedUsers can view log files.

Viewing log files

The Network Security console now provides a view of the log files easily.

To view log files

- 1 In the Network Security console, click **Admin > Node > Manage Logs**.
- 2 In **Select Node**, choose a node from the pull-down list, and click **OK**.
- 3 In **Log Files**, do one of the following:
 - Click a log file to select it.
 - Click **Refresh Table** to get the latest logs.
- 4 In **Actions**, click **View**.
- 5 In **View Log**, do any or all of the following:
 - Scroll to read all lines on the log.
 - In the **Operational Log** tab, view the log.
 - In the **Events** tab, view the events.
 - In **Go To Page**, enter a page number.

- Click **Next Page** to progress forward.
 - Click **Previous Page** to progress backward.
- 6 Click **Close** to exit.

Note: Both StandardUsers and RestrictedUsers can view log files.

Viewing live log files

The Network Security console now provides a view of the live log files easily.

To view live log files

- 1 In the Network Security console, click **Admin > Node > Manage Logs**.
- 2 In **Select Node**, choose a node from the pull-down list, and click **OK**.
- 3 In **Log Files**, do one of the following:
 - Click a log file to select it.
 - Click **Refresh Table** to get the latest logs.
- 4 In **Actions**, click **View Live Log**.
- 5 In **Live Log**, scroll to read all lines on the log.
- 6 Click **Close** to exit.

Note: Both StandardUsers and RestrictedUsers can view live log files.

Refreshing the list of log files

The Network Security console now provides a way to update the view after each change to the log file table.

To refresh the table

- 1 In the Network Security console, click **Admin > Node > Manage Backups**.
- 2 In **Select Node**, choose a node from the pull-down list, and click **OK**.
- 3 In **Logs**, click **Refresh Table**.

Note: Both StandardUsers and RestrictedUsers can refresh the log files table.

Index

Numerics

7100 Series. *See* appliances

A

accounts

about user logins 27

adjusting

view by columns 69

view of policies 68

administration console. *See* Network Security console

administration service

node architecture 29

Administrator

pre-defined login account 103

alert manager

node architecture 29

alerting. *See* logging

alerts. *See* notifications

analysis

about 24

about cross-node correlation 25

about event correlation 24

about event responses 29

about refinement rules 24

about Smart Agents 31

about the architecture 29

assigning priority level 77

annotating

entire policies 71

event instances 72

event types in a policy 71

appliances

about 31

about blocking 32

about detection 32

about in-line mode 32

about interface groups 32

about LCD panel 38

about nodes 52

about passive mode 32

about response 32

about serial console 39

about the 7100 Series 9

documentation 14

fail-open 33

management via consoles 38

monitoring interfaces 57

single-node deployment 42

viewing in-line pairs 58

viewing interface groups 57

viewing nodes 55

architecture

about the core 19

about the management and detection 26

about the node 28

FlowChaser 31

attack responses. *See* responses

attacks

categories 77

definition 99

flood-based 80

target IP address 97, 100

Auto Update tab

about 67

automated

response architecture 74

B

blocking rules

about 32

bypass unit. *See* in-line

C

clusters

about deployment 40, 43

monitoring groups 44

subclusters 44

tracking data stream 80

columns

adjusting the view of event types 69

- selecting 100
- communication
 - via QSP proxy 29
- confidence
 - about level 78
 - likelihood of attack 78
 - mapping level 101
 - response rules 78
- console response action
 - configuring 82
- console. *See* Network Security console, serial console, Symantec Decoy Server console, LCD panel
- copy ports. *See* monitoring interfaces
- correlation
 - about 24
 - about cross-node analysis 25
- custom response actions
 - creating rules 81
 - failure to execute 103
- custom signatures. *See* user-defined signatures

D

- data
 - events displayed 97, 100
 - incidents 96
 - tracking stream 80
- databases
 - architecture 29
 - time delay while loading 36
- deception
 - device objects 63
- Decoy Server. *See* Symantec Decoy Server
- denial of service. *See* DoS
- deployment
 - about 40
 - about clusters 40
 - about in-line mode 40
 - about passive mode 40
 - about single-node 40
 - monitoring groups 44
 - node clusters 43
 - single appliance node 42
 - single node 41
 - single software node 41
- details
 - viewing event types 70
 - viewing objects 50
- detection

- about 85
- about 7100 Series appliances 32
- about architecture 20
- about denial of service 23
- about protocol anomaly detection 85
- about refinement rules 86
- about signature 86
- about traffic rate monitoring 23
- about user-defined signatures 22
- by refinement rules 89
- external EDP 23
- port mapping 87
- protocol anomaly 21
- signature 87
- Symantec signatures 22, 88
- user-defined signatures 88
- viewing port mappings 87
- viewing signatures 89

Devices

- viewing details 92

devices

- event data display 97, 100
- event notice display 102

documentation

- 7100 Series 14
- software 15

DoS

- about detection architecture 23
- top Telnet event type 111

drill-down reports

- destination sources 114
- devices with flow statistics 115
- drill-down-only reports 116
- event destinations 116
- event details 116
- event lists 116
- event sources 116
- events per day 113
- events per hour 113
- events per month 113
- flows by destination address 116
- flows by destination port 117
- flows by protocol 117
- flows by source address 116
- flows by source port 117
- incident details 116
- incidents list 112
- incidents per day 112
- incidents per hour 112

- incidents per month 112
- source destinations 114
- top events 111
- top level 110

E

- editing
 - user passphrases 39
- EDP
 - about Event Dispatch Protocol 23
 - detection architecture 23
- email
 - initiation request failure 103
 - notification failure 103
 - notification messages 80
- errors
 - email initiation request failure 103
 - email notification failure 103
 - SNMP alert failure 103
 - SNMP initiation request failure 103
 - truncated SNMP message 103
- ESP
 - about node architecture 30
- ethernet
 - sensor interface media type 93
- Event Dispatch Protocol. *See* EDP
- event source
 - response rules 78
- event target
 - response rules 76
- event types 77
 - adjusting the view by columns 69
 - searching response rules 76
 - viewing details 70
- events
 - about event dispatch protocol 23
 - about event stream provider. *See* ESP
 - annotating 95
 - annotating an instance 72
 - annotating policies 71
 - customizing responses 81
 - data displayed 97, 100
 - definition 99
 - destination report 116
 - detail reports 116
 - email notifying 80
 - filtering 98, 101
 - filtering tables 98, 101
 - list reports 116

- modifying the view 38
- modifying the view of types 38
- next action parameter 79
- none option 80
- notice 102
- priority color coding 95
- reporting
 - per day 113
 - per hour 113
 - per month 113
- response parameter 79
- searching for types 68
- selecting columns 100
- SNMP notification 80
- sorting by classful destination 113
- sorting by classful source 114
- sorting by protocol 114
- sorting by vendor 114
- source parameter 78
- source reports 116
- target parameter 76
- top destinations 111
- top report type 111
- top sources 111
- TrackBack function 80
- type parameters 77
- viewing 99
- export flow action
 - response rules 82

F

- fail-open
 - about 33, 42
- failures
 - See also* errors
- filters
 - applying to incident tables 98, 101
 - ignoring attacks 80
 - preserving incidents during fail-over 99
 - See also* drop filter
 - showing incidents from selected nodes 99
 - showing operational events 98
- flow alert rules
 - viewing 83
- FlowChaser
 - about 31
- flows
 - about querying 117
 - alert rules 83

- devices with statistics 115
- replaying traffic 84
- reports by destination address 116
- reports by destination port 117
- reports by protocol 117
- reports by source address 116
- reports by source port 117
- traffic playback tool 83
- viewing current 117
- viewing exported 119

formats

- report 110

Full Event List tab

- about 67

G

groups

- about interface groups 32
- about monitoring groups 44
- about user login accounts 39

H

Hardware Compatibility Reference

- viewing 16

host name

- viewing destination IP 105
- viewing source IP 105

I

incidents

- annotating events 95
- cross-node details 104
- data 96
- definition 99
- details 104, 116
- filtering 98, 101
- list 112
- marking as viewed 95
- modifying the view 38
- priority color coding 95
- reporting per day 112
- reporting per hour 112
- reporting per month 112
- selecting columns 100
- viewing from monitoring groups 44

in-line

- about 10, 32, 42

- about bypass unit 11, 33
- about deployment 40
- about fail-open 33
- sensor processes 30
- viewing in-line pairs 58
- viewing interface groups 57

in-line pairs

- on appliance nodes 56
- viewing 58

interface groups

- about 32, 42
- on appliance nodes 56
- viewing 57

interfaces

- about 7100 Series appliance 56
- about Smart Agents 61
- monitoring on software nodes 53
- viewing sensor details 93

K

Knowledge Base

- viewing 16

L

LCD panel

- about 38

loading

- events button 104

logging

- about 32
- about install logs 121
- about log files 121
- about operational logs 122
- refreshing the view 123
- viewing live logs 123
- viewing log files 122

login

- from Windows 36
- history report 115
- Network Security Administrator 103
- Network Security console 103

logs

- about 121
- about install 121
- about operational 122
- managing 122
- refreshing the list 123
- viewing 122

viewing live 123

M

management console. *See* Network Security console

managers

- alert 29
- sensor 29

managing

- from the Network Security console 36
- user login accounts 39
- user passphrases 39
- via user interfaces 35

mapping

- base event to event type 104
- base event to priority event 104
- event type to incident 112
- network sample 41
- viewing port 87

master nodes

- primary default 52
- viewing appliance 55

modes

- about alerting 32
- about blocking 32
- about cluster 40
- about in-line 32, 40
- about passive 40
- about passive mode 32
- about single-node 40, 41

monitoring

- traffic rate 23

monitoring groups

- choosing view 44
- deploying 44

monitoring interfaces

- on appliance nodes 56
- on software nodes 53
- viewing on appliance nodes 57
- viewing on software nodes 54

N

Network Security

- accessing the Network Security console 36
- logging in 103
- logging in as Administrator 103
- login history 115

Network Security console

- about 26

accessing 36

changing font size 38

choosing view 37, 38

expanding or collapsing view 37

launching from Windows 36

login 36

node status indicator 38

viewing 37

Network Security node

about alert manager architecture 29

QSP proxy architecture 29

sensor manager architecture 29

Network Security nodes

about 52

networks

sample topology map 41

viewing advanced options 52, 55

next action

- configuring 79
- response rules 79

nodes

about appliances 31

about cross-node correlation 25

about Network Security nodes 52

administration service architecture 29

cluster deployment 43

database architecture 29

incident details 104

modifying the view 37

monitoring groups 44

monitoring interfaces on software nodes 54

single-node deployment with appliance 42

single-node deployment with software

nodes 41

status indicator 38

viewing 7100 Series appliance nodes 55

viewing details 92

viewing Devices tab 37

none option

about 80

Notes tab

annotating policies 68

notifications

about alert manager 29

configuring email 80

O

objects

- viewing 51

- viewing details 50
- operational logs
 - about 122
- options
 - about 80
 - viewing advanced network 52, 55

P

- packets
 - enabling capture mode 93
- PAD
 - about 85
- panel
 - LCD 38
- parameters
 - event source 78
 - event target policy 76
 - event type 77
 - response rules 76, 79
 - viewing sensors 87
- passive mode
 - about 32
 - sensor processes 30
- passive modes
 - about deployment 40
- passphrases
 - editing 39
 - managing 39
- patches
 - accessing sites 16
- policies
 - about 25
 - about protection 65
 - adjusting the view 68
 - annotating 71
 - Auto Update tab 67
 - column view 69
 - Full Event List tab 67
 - modifying the view 38
 - Notes tab 68
 - Protection Policies tab 67
 - Search Events tab 67
 - searching event types 68
 - understanding the workarea 67
 - updating 70
 - viewing 66
 - viewing event type details 70
- port mapping
 - about 87

- ports
 - flow reports by destination 117
 - flow reports by source 117
 - mapping 87
 - viewing mappings 87
 - viewing port mappings 87
- portscan
 - top event type 111
- primary
 - default master node 52
- priority
 - color coding 95
 - configuring levels 77
 - mapping level 101, 105
- processes
 - about sensors 30
- ProductUpdates
 - accessing 16
- protection policies
 - about 25, 65
 - adjusting the view 68
 - annotating 71
 - Auto Update tab 67
 - column view 69
 - Full Event List tab 67
 - Notes tab 68
 - Protection Policies tab 67
 - Search Events tab 67
 - understanding the workarea 67
 - updating 70
 - using Search Events 68
 - viewing 66
 - viewing event type details 70
- Protection Policies tab
 - about 67
- protocol anomaly detection. *See* PAD
- protocols
 - about anomaly detection architecture 21
 - EDP 23
 - flow 115
 - flow reports by 117
 - list of events 114
 - viewing mappings to supported 87
 - watching for anomalies 87

Q

- QSP
 - query service proxy. *See* QSP
 - secure communication 29

- queries
 - replaying traffic flow data 84
 - traffic playback tool 83
- querying

- current flows 117
 - exported flows 119
 - policy event type list 76

R

- refinement
 - about 24
 - detection rules method 86, 89
- reliability

- assigning levels 105
 - mapping level 105

- reports

- console 109
 - format 110
 - querying flows 117
 - replaying traffic flow 84
 - top level 110
 - traffic playback 83
 - viewing current flows 117
 - viewing exported flows 119

- response actions

- enabling console 82
 - response rules 78
 - TCP reset 81

- response rules 77

- about automated 25
 - color coding 75
 - configuring console response 82
 - custom response 81
 - event source parameters 78
 - event target parameter 76
 - event type parameters 77
 - export flow action 82
 - next action parameter 79
 - none option 80
 - parameters 76
 - response parameter 79
 - searching for event types 76
 - setting confidence levels 78
 - setting event sources 78
 - setting event targets 76
 - setting event types 77
 - setting next actions 79
 - setting response actions 78
 - SNMP notification 80

- TCP reset 81
 - TrackBack 80
 - viewing 75

- responses

- about 25
 - about automated 74
 - about parameters 76
 - assigning priority levels 77
 - automated 74
 - configuring confidence level 78
 - configuring priority 77
 - customizing responses 81
 - email notifications 80
 - enabling automatic next action 79
 - failure of custom 103
 - flow alert rules 83
 - none option 80
 - setting parameters 79
 - SNMP notifications 80
 - tracking data stream to source 80
 - traffic record 81
 - viewing port mappings 87
 - viewing rules 75

- RestrictedUser

- pre-defined login account 103

- roles

- about administration of 27

- routers

- viewing 59

- rules

- about refinement 24
 - flow alert 83
 - refinement detection 86, 89

S

- Search Events tab

- about 67
 - creating a subset of event types 68

- sensor manager

- node architecture 29

- sensors

- about node architecture 30
 - about sensor processes 30
 - viewing interface details 93
 - viewing parameters 87

- serial console

- about 39

- severity 77

- mapping level 101, 105

- signatures
 - about 22
 - about detection 86
 - about user-defined 22
 - detection by 87
 - Symantec 22, 88
 - user-defined 88
 - variables 89
 - viewing 89
- slave nodes
 - synchronizing 52
 - viewing appliance 55
- Smart Agents
 - about 31
 - about interfaces 61
- sniffer. *See* sensor processes
- SNMP
 - alert failure 103
 - configuring notification 80
 - request failure 103
 - truncated message 103
- software
 - about nodes 52
 - about the node architecture 28
 - accessing Knowledge Base 16
 - documentation 15
 - viewing Hardware Compatibility Reference 16
- source
 - destination reports 114
- StandardUser
 - pre-defined login account 103
- standby nodes
 - about failover 43
- stateful signatures. *See* signatures
- statistics
 - devices with flow 115
- stopping
 - end time 105
 - incident response 80
- Symantec Decoy Server
 - enable via Symantec Network Security 63
 - external sensors 63
- Symantec Network Security
 - about analysis 24
 - about database architecture 29
 - about detection 20
 - about response 25
 - about software features 11
 - about the 7100 Series 9

- about the core architecture 19
- about the node architecture 28
- accessing patch site 16
- accessing the Network Security console 36
- detection architecture 26
- enabling Symantec Decoy Server 63
- management architecture 26
- software documentation 15
- Symantec signatures. *See* signatures
- synchronizing
 - slave nodes 52
- synflood
 - top event type 111

T

- tabs
 - about Advanced Network Options tab 52, 55
 - about Auto Update tab 67, 70
 - about Devices tab 27
 - about Full Event List tab 67
 - about Incidents tab 27
 - about Notes tab 68, 71
 - about Policies tab 27
 - about Protection Policies tab 66, 67
 - about Search Events tab 67, 68
- TCP reset 81
- third-party integration
 - Smart Agents 31
- tool tips
 - annotating policies 71
- topology
 - about network 51
 - modifying the view 37
 - viewing 37
 - viewing device objects 49, 50
- TrackBack
 - about 12, 13
 - configuring 80
- traffic
 - about rate monitoring 23
 - playback tool 83
 - record response 81
 - replaying recorded 84
 - viewing current flows 117
 - viewing exported flows 119

U

- updating

- protection policies 70
- user login accounts
 - establishing 39
- user-defined signatures
 - about 22
- users
 - about administration of 27
 - editing passphrases 39
 - login history 115
 - Network Security console login 103

V

- variables
 - signatures 89
- viewing
 - adjusting policies 68
 - changing font size 38
 - color-coded response rules 75
 - expanding and collapsing the view 37
 - flow alert rules 83
 - in-line pairs 58
 - interface groups 57
 - live logs 123
 - log files 123
 - logs 122
 - monitoring groups 44
 - monitoring interfaces on appliance nodes 57
 - monitoring interfaces on software nodes 54
 - monitoring interfaces to software nodes 54
 - Network Security console 37
 - object details 50
 - objects 51
 - response rules 75
 - routers 59
 - sensor parameters to objects 87
 - topology 37, 38
- VLAN
 - specifying rules 78

W

- Windows
 - launching Network Security console 36

